03S0944

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００２年１０月２２日

出願番号
Application Number: 特願２００２－３０７５７６

[ST. 10/C]: [ＪＰ２００２－３０７５７６]

出願人
Applicant(s): 株式会社東芝

２００３年　７月　８日

特許庁長官
Commissioner,
Japan Patent Office 太田信一郎

出証番号　出証特２００３－３０５３９９４

【書類名】　特許願
【整理番号】　A000205008
【提出日】　平成14年10月22日
【あて先】　特許庁長官　殿
【国際特許分類】　G06F　7/00
【発明の名称】　情報共有支援装置および情報共有支援方法
【請求項の数】　9
【発明者】
【住所又は居所】　神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内
【氏名】　土井　美和子
【特許出願人】
【識別番号】　000003078
【氏名又は名称】　株式会社　東芝
【代理人】
【識別番号】　100058479
【弁理士】
【氏名又は名称】　鈴江　武彦
【電話番号】　03-3502-3181
【選任した代理人】
【識別番号】　100084618
【弁理士】
【氏名又は名称】　村松　貞男
【選任した代理人】
【識別番号】　100068814
【弁理士】
【氏名又は名称】　坪井　淳

【選任した代理人】
　【識別番号】　100092196
　【弁理士】
　【氏名又は名称】　橋本　良郎
【選任した代理人】
　【識別番号】　100091351
　【弁理士】
　【氏名又は名称】　河野　哲
【選任した代理人】
　【識別番号】　100088683
　【弁理士】
　【氏名又は名称】　中村　誠
【選任した代理人】
　【識別番号】　100070437
　【弁理士】
　【氏名又は名称】　河井　将次
【手数料の表示】
　【予納台帳番号】　011567
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　情報共有支援装置および情報共有支援方法

【特許請求の範囲】

【請求項１】

情報提供者から、人物の顔などを含む映像情報、脈拍や体温などの生体情報などの第１の情報を取得する取得手段と、

この取得手段で取得した第１の情報に、少なくとも当該第１の情報にアクセス可能な情報利用者を限定するためのアクセス権のレベルを定めたレベル情報を含む付加情報を付加して記憶するとともに、当該第１の情報を提供した前記情報提供者に関する個人情報を記憶する第１の記憶手段と、

この第１の記憶手段に記憶された前記第１の情報と、当該第１の情報に対応する個人情報との間の対応関係を記憶する第２の記憶手段と、

前記第１の記憶手段に記憶された第１の情報および当該第１情報に対応する個人情報のうちの少なくとも一方へアクセスするためのアクセス要求を受信する受信手段と、

前記アクセス要求の要求元である情報利用者に対し予め定められたアクセス権のレベルが前記第１の情報にアクセス可能なときに当該秘第１の情報を提供し、当該アクセス権のレベルが前記個人情報にアクセス可能なときには、前記第２の記憶手段に記憶された対応関係に基づき、当該個人情報を前記第１の記憶手段から読み出して当該個人情報を提供する情報提供手段と、

を具備したことを特徴とする情報共有支援装置。

【請求項２】

個人情報を含む第１の情報を取得する取得手段と、

この取得手段で取得した第１の情報から前記個人情報を抽出する抽出手段と、

前記取得手段で取得した第１の情報から前記抽出手段で抽出した個人情報を分離することにより、匿名化情報を生成する生成手段と、

この生成手段で生成された匿名化情報に、少なくとも当該匿名化情報に対応する個人情報にアクセス可能な情報利用者を限定するためのアクセス権のレベルを定めたレベル情報を含む付加情報を付加して記憶するとともに、前記個人情報を

記憶する第１の記憶手段と、

この第１の記憶手段に記憶された前記匿名化情報と、当該匿名化情報に対応する個人情報との間の対応関係を記憶する第２の記憶手段と、

前記第１の情報のへアクセスするためのアクセス要求を受信する受信手段と、

前記アクセス要求の要求元である情報利用者に対し予め定められたアクセス権のレベルが前記個人情報にアクセス不可能なときには、前記第１の記憶手段から前記アクセス要求に対応する前記第１の情報の匿名化情報を読み出して、当該匿名化情報を提供し、当該アクセス権のレベルが前記個人情報にアクセス可能なときには、前記第２の記憶手段に記憶された前記対応関係に基づき、さらに、当該第１の情報に対応する個人情報を前記第１の記憶手段から読み出して、当該個人情報と当該匿名化情報とから前記第１の情報を生成して当該第１の情報を提供する情報提供手段と、

を具備したことを特徴とする情報共有支援装置。

【請求項３】

前記情報提供者への情報提供に対する第１の料金の支払いを行うとともに、前記情報利用者から前記情報提供手段で提供した情報に応じた第２の料金の徴収を行うための課金手段と、

をさらに具備したことを特徴とする請求項１記載の情報共有支援装置。

【請求項４】

前記取得手段で取得した第１の情報に付加する付加情報には、前記レベル情報の他、さらに、当該第１の情報に含まれる情報の種別、当該第１の情報の取得日時、当該第１の情報の暗号化方法のうちの少なくとも１つを含み、

前記第１の情報に複数種類の情報が含まれているときには、当該複数種類の情報間の関連付けを行うことを特徴とする請求項１記載の情報共有支援装置。

【請求項５】

前記第２の記憶手段は、前記前記第１の情報の第１の識別子と前記個人情報の第２の識別子との対応関係を記憶することを特徴とする請求項１記載の情報共有支援装置。

【請求項６】

前記第２の記憶手段は、前記匿名化情報の第１の識別子と前記個人情報の第２の識別子との対応関係を記憶することを特徴とする請求項２記載の情報共有支援装置。

【請求項７】

前記生成手段は、前記取得手段で取得した第１の情報から前記抽出手段で抽出した個人情報に対応する部分を削除する、あるいはモザイク化する、あるいは当該個人情報に対応する部分を他の情報に置き換えることにより、前記匿名化情報を生成することを特徴とする請求項２記載の情報共有支援装置。

【請求項８】

情報提供者から、人物の顔などを含む映像情報、脈拍や体温などの生体情報などの第１の情報を取得し、当該第１の情報に、少なくとも当該第１の情報にアクセス可能な情報利用者を限定するためのアクセス権のレベルを定めたレベル情報を含む付加情報を付加して第１の記憶手段に記憶するとともに、当該第１の記憶手段に当該第１の情報を提供した前記情報提供者に関する個人情報を記憶し、この第１の記憶手段に記憶された前記第１の情報と、当該第１の情報に対応する個人情報との間の対応関係を第２の記憶手段に記憶し、

前記第１の記憶手段に記憶された第１の情報および当該第１情報に対応する個人情報のうちの少なくとも一方へアクセスするためのアクセス要求を受信したとき、当該アクセス要求の要求元である情報利用者に対し予め定められた、アクセス権のレベルが前記第１の情報にアクセス可能なときには当該第１の情報を提供し、当該アクセス権のレベルが前記個人情報にアクセス可能なときには、前記第２の記憶手段に記憶された対応関係に基づき、当該個人情報を前記第１の記憶手段から読み出して当該個人情報を提供することを特徴とする情報共有支援方法。

【請求項９】

個人情報を含む第１の情報を取得して、当該第１の情報から前記個人情報を抽出し、当該第１の情報から前記抽出した個人情報を分離することにより、匿名化情報を生成し、

この生成された匿名化情報に、少なくとも当該匿名化情報に対応する個人情報にアクセス可能な情報利用者を限定するためのアクセス権のレベルを定めたレベ

ル情報を含む付加情報を付加して第１の記憶手段に記憶するとともに、当該第１の記憶手段に前記個人情報を記憶し、この第１の記憶手段に記憶された前記匿名化情報と、当該匿名化情報に対応する個人情報との間の対応関係を第２の記憶く手段に記憶し、

前記第１の情報のへアクセスするためのアクセス要求を受信したとき、前記アクセス要求の要求元である情報利用者に対し予め定められたアクセス権のレベルが前記個人情報にアクセス不可能なときには、前記第１の記憶手段から前記アクセス要求に対応する前記第１の情報の匿名化情報を読み出して、当該匿名化情報を提供し、当該アクセス権のレベルが前記個人情報にアクセス可能なときには、前記第２の記憶手段に記憶された前記対応関係に基づき、さらに、当該第１の情報に対応する個人情報を前記第１の記憶手段から読み出して、当該個人情報と当該匿名化情報とから前記第１の情報を生成して当該第１の情報を提供することを特徴とする情報共有支援方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、ユーザの個人情報を守秘しつつ、収集した情報を利用したデータマイニングなどを円滑に行うことのできる情報共有支援装置に関する。

【０００２】

【従来の技術】

近年、コンピュータが目に見えない形で、いたるところに遍在する状況になっている。日常生活を支援するユビキタスコンピューティング(ubiquitous computing)や、これをネットワークでつなげたユビキタスネットワークの研究が活発化している。

【０００３】

例えば、２００５年までに、超小型チップネットワーキングプロジェクト、何でもマイ端末プロジェクト、どこでもネットワークプロジェクトの３つのプロジェクトを推進し、ユビキタスネットワークの要素技術を確立するとしている（例えば、非特許文献１参照）。

【０００４】

超小型チップネットワーキングプロジェクトでは、砂粒大の超小型チップにより、１００億個の端末が協調・制御するネットワーク技術の実現をめざしている。

【０００５】

またなんでもマイ端末プロジェクトでは、ワイヤレスＩＣカードをかざすと瞬時にどんな端末でも自分の端末として利用することをめざし、従来の1万分の１以下のリアルタイムな応答・認証が可能なネットワーク技術を実現しようとしている。

【０００６】

さらに、どこでもネットワークプロジェクトでは、どこにいても１００Ｍｂｐｓで１００万人が同時に利用できるようにして、いつでもネットワークが繋がり、オフィスと同一の通信サービス環境が創出できることをめざしている。

【０００７】

一方、現実の世界では、携帯電話にGPS（Global Positioning System）がついたり、あるいはPHSでは、電波の強度により基地局からの距離を推定したりすることで、ユーザの位置を特定し、その位置に応じて、道案内などの情報提供を行うことができるようになっている。実際に、徘徊老人や塾に通う子供にもたせ、保護者や家族などあらかじめ登録された携帯電話からは、リアルタイムに相手の位置を取得できるサービスもはじまっている。

【０００８】

既に、カーナビゲーションでは、GPSとジャイロにより車の位置（緯度,経度）を測定し、それにより、地図を表示し、目的地までの経路を案内するものである。

【０００９】

一方、ＥＣＨＯＮＥＴなど家庭内にネットワークを張り巡らし、省電力や監視を行う情報家電ネットワークの開発も、さかんに行われている。脂肪体重計にＩｒＤＡがついていて、体重を量ると自動的にネットワークを通じて、パソコンに計測した体重と脂肪率が送られるような体重計も製品化されている。トイレを使

用すると、体重や血圧、脈拍、血糖値が計測され、それがネットワークを通じて、健康管理センターなどに送るホームヘルスケアのシステムが開発されている。開発されたホームヘルスケアシステムの実証実験などに関しても、予防医学の観点から、国家的な取り組みが行われている。

【００１０】

加速度センサーが小型化して、高性能の万歩計が製品化されてきている。万歩計で計測したデータを、USB（Universal Serial Bus）を介してパソコンで管理することができるものも製品化されている。

【００１１】

また、鉄道会社により、非接触ＩＣカードによるプリペードカードと定期券をあわせたサービスが、２００２年より大々的に開始されている。定期券とあわせたサービスでは、非接触ＩＣカード定期券の所有者が特定できるので、サービス提供業者である鉄道会社は、自社鉄道に限定されるとはいえ、非接触ＩＣカード定期券所有者の移動行動をすべて、時刻付きで把握することが可能となっている。

【００１２】

また、凶悪犯罪の増加に対抗し、銀行のＡＴＭ、コンビニ店内、繁華街、高層マンションのエレベータホールあるいはエレベータの籠内などに、数多くの防犯／監視カメラが設置されている。これらの監視カメラでは、１～１０秒間隔ごとに２４時間撮影し続けるものである。実際に犯罪などが起こった場合に、警察などに対して、記録画像を提供するといった運営が行われている。

【００１３】

これに対し、同じ監視カメラでも、国土交通省が河川の水位や雨量を観察するために設置しているカメラの映像は、ケーブルＴＶやＷｅｂなどを通じて、一般に公開されている。ケーブルＴＶは、ケーブルＴＶ加入者だけへのサービスであるので、有料である。しかし、１０分間隔ではあるが、無料でリアルタイムに見ることができるものもある（例えば、非特許文献２参照）。

【００１４】

一方、最近は犯罪増えたために、塾帰りの子供が無事かどうかの安否を確認し

たいという要望が親にはある。子供の所在地がわかっていれば、その付近にある監視カメラを使って、現在の子供の様子をみることは技術的には可能である。あるいは、単に、これから出かけようとする場所の混雑度合いを、監視カメラの映像などを使って確認することも、可能である。このようなときに、問題となるのは、街角などの他の歩行者の映像も一緒に写りこんでしまうことである。歩行者は街頭カメラの映像は犯罪時にしか使用されないとおもっているので、他の目的に使用されると、肖像権侵害になる恐れがある。

【００１５】

また、最近では、携帯電話についているＩｒＤＡを使って、個人認証をおこなったり、着メロのダウンロードをおこなったりするようなサービスも出ている。あるいは携帯電話の公衆網への接続回線を使って、電子的にチケットをダウンロードし、これをバーコードでの呈示、あるいはＩｒＤＡでの送信を行うことで、電子的に改札を行う方法も考えられている。あるいは、ＩｒＤＡ経由で個人認証をおこない、その後、携帯電話にあらかじめチャージされている電子マネーを引き落とすような、電子マネーへの展開も検討されている。この場合、クレジットカードやポイントカードなどと同様に、携帯電話、あるいはクレジットカード、ポイントカードの持ち主が、いつ、どこで、何を購買したかが、店舗側のサーバーにすべて蓄積されている。店舗側は、このデータを使って、例えば、20代女性の間で、どのような商品が人気があるのか、次にはどのような商品を用意すべきかといった、ＣＲＭ(Customer Relation Management)をおこないたい。

【００１６】

以上のように、防犯あるいは健康管理などの種々の観点から、カメラや生体センサなどの、実に様々なセンシング機器が、銀行や駅、コンビニ、繁華街などの公共の場所や、家庭などの私的な場所に設置されたり、あるいは個人に装着されたりするようになっている。

【００１７】

家庭内のデータは、現状ではホームサーバーなどに蓄積管理する方向である。トイレや、装着している健康管理機器とホームサーバー間の通信は、無線ＬＡＮ(Local Area Network)やＩｒＤＡ、Ｂｌｕｅｔｏｏｔｈなどでワイヤレスに行う

方向である。さらに蓄積先のホームサーバーはＡＤＳＬなどのブロードバンドネットワークに、24時間接続し続ける方向である。現状では、個人家庭に有用なデータがないため、個人のホームサーバーへのハッキングやＤＯＳ攻撃などは、まだまだ行われていない。しかし、情報家電が浸透し、ホームサーバーに非常に多くのデータが蓄積されるようになると、今後は、ホームサーバーを目指したハッキングが増加する可能性が非常に高い。

【００１８】

このため、利用者は、ネットワークへの接続に不安を抱いている。ハッキングからホームサーバーのデータを守るために、ファイアウオールを導入すればよいのであるが、ネットワークに関する知識がない利用者にとっては、ファイアウオールの導入もままならない。そのままでは、安心してネットワークにつなげることができない。

【００１９】

一方、医療機関は、糖尿病患者の血糖値を管理するだけでなく、予防医学の観点から、生活習慣病予備群を含めた大量のデータを収集し、マイニングし、治療や健康指導に役立てたいとの希望をもっている。患者は自分のデータを閲覧できるのは、自分と担当医に限りたい。自分のデータが予防医学に役立つとしても、自分の名前が出るのが困る。予防医学の研究などに使われる際には、プライバシーにかかわる情報は完璧に削除して、「35歳女性　身長163cm　体重48kg　血圧116　72　…」といったように研究に必要な情報のみに抽象化して欲しいと考えている。

【００２０】

しかし、現状では、このように個人情報の秘匿を行うような作業は、研究に利用する医師に任されている。医師がファイやウオールなどの情報保護に関する知識や、情報秘匿化のためのプログラミングなどが行える場合は少ない。また、そのような知識や能力があったとしても時間が足りず、十分なケアを行うことができない場合がほとんどである。

【００２１】

同様に、コンビニやスーパーマーケットなどの流通業界では、年代・性別ごと

にどのような商品が購買されているのかを知り、次の商品の仕入れに役立てたい。コンビにでは、現在、決済の際に、店員が顧客をみて類推して、「中年・男性」などと入力を行っている。これが、ポイントカードや携帯電話による決済になれば、これらのデータを自動的に取得できるので、便利となる。

【００２２】

一方、鉄道会社は、非接触ICカード定期により、乗降客の流れを把握できるので、このデータに基づいて列車の運行計画や、駅設備の改善を行うことができる。しかし、非接触ICカード定期利用者は、自分のデータが利用されているとしても、個人情報としては、保護されていることを期待している。

【００２３】

【非特許文献１】

“何でもどこでもネットワークの実現に向けて”、[online]、総務省の「ユビキタスネットワーク技術の将来展望に関する調査研究会」、［平成１４年１０月８日検索］、インターネット＜ＵＲＬ：http://www.soumu.go.jp/s-news/2002/pdf/020611_4_1.pdf＞

【００２４】

【非特許文献２】

京浜工事事務所トップページ、［online］、［平成１４年１０月８日検索］、インターネット，＜ＵＲＬ：http://www.keihin.ktr.mlit.go.jp/index_top.html＞

【００２５】

【発明が解決しようとする課題】

街頭カメラの映像や鉄道の利用情報、個人の生体情報、個人の購買情報など、従来、コンテンツとして、明確に意識して扱われなかった情報が、大量に電子化され、ネットワークを通じた流通が可能となってきている。個人はこれらのデータを保護したいと考え、一方、企業、鉄道会社、医療機関、流通業界などは、データマイニングをしてマーケティングや設備投資などへの基礎データとして利用したいと考えている。このように双方の利害が相反している。

【００２６】

このように、従来は、個人情報を含む情報や、各個人に関わる個人情報に対応付けられた当該個人情報に準ずる生体情報や購買情報などの情報を個人情報を保護しつつ、異なる目的で有効に利用を図るための環境がないという問題点があった。

【００２７】

そこで、本発明は、上記問題点に鑑み、個人情報を含む情報や、各個人に関わる個人情報に対応付けられた当該個人情報に準ずる生体情報や購買情報などの情報を個人情報を保護しつつ、各種目的で他人に有効に利用させることができる情報共有支援方法およびそれを用いた情報共有支援装置を提供することを目的とする。

【００２８】

【課題を解決するための手段】

（１）本発明は、情報提供者から、人物の顔などを含む映像情報、脈拍や体温などの生体情報などの第１の情報を取得し、当該第１の情報に、少なくとも当該第１の情報にアクセス可能な情報利用者を限定するためのアクセス権のレベルを定めたレベル情報を含む付加情報を付加して第１の記憶手段に記憶するとともに、当該第１の記憶手段に当該第１の情報を提供した前記情報提供者に関する個人情報を記憶し、この第１の記憶手段に記憶された前記第１の情報と、当該第１の情報に対応する個人情報との間の対応関係を第２の記憶手段に記憶し、前記第１の記憶手段に記憶された第１の情報および当該第１情報に対応する個人情報のうちの少なくとも一方へアクセスするためのアクセス要求を受信したとき、当該アクセス要求の要求元である情報利用者に対し予め定められた、アクセス権のレベルが前記第１の情報にアクセス可能なときに当該第１の情報を提供し、当該アクセス権のレベルが前記個人情報にアクセス可能なときには、前記第２の記憶手段に記憶された対応関係に基づき、当該個人情報を前記第１の記憶手段から読み出して当該個人情報を提供することを特徴とする。

【００２９】

本発明によれば、生体情報や人物の画像などを取得した時点で、この取得した情報と、当該取得した情報とは別個に取得した個人情報とは分離して記憶する。

従って、後に情報利用者に個人情報以外の情報を提供する際には、提供した情報からは個人情報を辿っていくことが不可能となる。このようにして、個人情報に関連付けられた生体情報などの情報であっても、他人からは当該個人情報にアクセスされることなく、当該生体情報を他者に利用させることが可能となり、個人のプライバシーを守って情報利用を有効に行うことができる。

【００３０】

好ましくは、前記第２の記憶手段は、前記前記第１の情報の第１の識別子と前記個人情報の第２の識別子との対応関係を記憶する。

【００３１】

（２）本発明は、個人情報を含む第１の情報を取得して、当該第１の情報から前記個人情報を抽出し、当該第１の情報から前記抽出した個人情報を分離することにより、匿名化情報を生成し、この生成された匿名化情報に、少なくとも当該匿名化情報に対応する個人情報にアクセス可能な情報利用者を限定するためのアクセス権のレベルを定めたレベル情報を含む付加情報を付加して第１の記憶手段に記憶するとともに、当該台１の記憶手段に前記個人情報を記憶し、この第１の記憶手段に記憶された前記匿名化情報と、当該匿名化情報に対応する個人情報との間の対応関係を第２の記憶手段に記憶し、前記第１の情報のへアクセスするためのアクセス要求を受信したとき、前記アクセス要求の要求元である情報利用者に対し予め定められたアクセス権のレベルが前記個人情報にアクセス不可能なときには、前記第１の記憶手段から前記アクセス要求に対応する前記第１の情報の匿名化情報を読み出して、当該匿名化情報を提供し、当該アクセス権のレベルが前記個人情報にアクセス可能なときには、前記第２の記憶手段に記憶された前記対応関係に基づき、さらに、当該第１の情報に対応する個人情報を前記第１の記憶手段から読み出して、当該個人情報と当該匿名化情報とから前記第１の情報を生成して当該第１の情報を提供することを特徴とする。

【００３２】

本発明によれば、人物の画像などの個人情報を含む情報を取得した時点で、この取得した情報に含まれる個人情報を抽出し、取得した情報を個人情報と、個人情報でない部分とに分離して記憶する。従って、所定のレベル以上のアクセス権

を持たない情報利用者には、個人情報部分は匿名化された匿名化情報を提供し、しかも、当該匿名化情報からは個人情報を辿っていくことは不可能となる。このようにして、個人情報とは切り離された匿名化された情報を提供することにより、個人情報を含むような情報であっても他人からは当該個人情報にアクセスされることなく、匿名化された情報を他者に利用させることが可能となり、個人のプライバシーを守って情報利用を有効に行うことができる。

【００３３】

なお、前記第２の記憶手段は、前記匿名化情報の第１の識別子と前記個人情報の第２の識別子との対応関係を記憶する。

【００３４】

また、取得した第１の情報から個人情報に対応する部分を削除する、あるいはモザイク化する、あるいは当該個人情報に対応する部分を他の情報に置き換えることにより、前記匿名化情報を生成する。

【００３５】

【発明の実施の形態】

以下、図面を参照して本発明の実施の形態を説明する。

（第１の実施形態）

図１に第１の実施形態にかかる情報匿名化システム１００の概略構成を示す。

【００３６】

センシング部１は、例えば、街頭カメラで撮影した画像（静止画、動画像を含む）や、図２に示したような装着者の脈拍や皮膚発汗（ＧＳＲ）、装着者の運動状態を表す加速度などの生体情報などを計測する端末装置である。

【００３７】

図２のセンシング部１は次のような働きをする。装着者がつける腕時計型のセンサモジュールには皮膚発汗、脈拍、加速度等のセンサがはいっており、これらの情報を例えば、１ｍｓｅｃ毎に計測する。計測した結果は、近距離無線Ｂｌｕｅｔｏｏｔｈ経由でＰＤＡ等の携帯通信端末に、例えば、５０ｍｓｅｃ毎に送信する。

【００３８】

皮膚発汗（ＧＳＲ）は、皮膚表面に汗をかくと、皮膚抵抗値が下がることを利用して、皮膚表面２点間の抵抗値を計ることで、皮膚発汗を計測するものである。緊張すると皮膚に発汗するので、皮膚発汗を緊張の度合いを示すものとして、嘘発見器などに使われている。

【００３９】

ＰＤＡ側では、これらの情報を解析し、歩行、走行、作業、安静、食事などの行動に沿って、「食後３０分です。薬を飲んでください」、「血糖値をはかりましたか」、などのアドバイスを行い、装着者の服用忘れ、計測忘れがないように、支援を行うようになっている。　センシング部１の構成は例えば、図３のようになっている。皮膚の抵抗値により皮膚発汗を測定する皮膚発汗測定部１２と、光電脈波センサなどにより脈拍を測定する脈拍測定１３と、２軸の加速度センサなどにより加速度を測定する加速度測定部１４とから構成される生体情報測定部１１と、その結果を無線で送信する通信部１５とから構成される。例えば、図３の生体計測部１１は、図２のセンサモジュールに対応し、図３の通信部１５は、図２のＰＤＡのような携帯型通信端末に対応する。

【００４０】

これら各測定部での皮膚温度、脈拍、ＧＳＲ、加速度などの測定結果（検知結果）は、図４に示すような生体情報として、出力される。ここでは、これら複数種類の生体情報が、通信部１５からセンシング情報として図１の送受信部４へ送信される。

【００４１】

実際に計測される皮膚温度、脈拍、ＧＳＲ、加速度のグラフを図４に示す。皮膚温度、脈拍、ＧＳＲ、加速度は、計測時刻に沿って、計測時刻と対応付けられて記憶される。加速度は分析されて、図４の下部に示すように、ＰＣ作業、座位、立位、歩行、走行などの行動に分析されている。

【００４２】

センシング部１は、ここでは、生体情報をセンシング情報として取得する場合を説明するが、この場合に限らず、生体情報以外の情報を取得するものであってもよい。

【００４３】

アクセス情報追加部２は、センシング部１が収集した情報を記録した後に当該情報にアクセスする際に用いる情報を追加したり、当該収集した情報から秘匿すべき個人情報を分離したりなどして、アクセス構造化情報記憶部３に記録する記録情報を作成するなどするものである。アクセス情報追加部２には、情報追加部２１と、情報関連化部２２と、情報匿名構造化部２３とからなっている。

【００４４】

情報関連化部２２は、センシング部１から複数種類のセンシング情報が出力されるときには、図４に示すように、計測時刻などにそって、複数のセンシング情報間の関連付けを行う。

【００４５】

情報追加部２１はセンシング情報の種別、情報取得日時、センシング情報の暗号化方法、センシング情報へアクセス可能な情報利用者を限定するためのアクセス権のレベルを表した情報（レベル情報）、当該センシング情報の情報提供者に関する情報などの付加情報の追加を行い、生体情報と当該付加情報とを含む記録情報を生成する。例えば、図４のように記録されたセンシング情報（ここでは、例えば生体情報）に対し、上記のような付加情報の追加を行った結果得られる各記録情報は、例えば、図５に示すような形式でアクセス情報構造化記憶部３に記憶される。アクセス情報構造化記憶部３は、センシング部１が収集した情報（センシング情報）とアクセス情報追加部２１が追加する付加情報とを対応させて（付加情報とセンシング情報とを一体化して）記憶する。例えば、ここではセンシング情報には、識別子「Ｂ１」、「Ｂ２」、…と付し、センシング情報自体は、例えば暗号化されて、付加情報とは別個にアクセス情報構造化記憶部３に記憶され、図５では、記録情報として、センシング情報の識別子と当該センシング情報に対応する付加情報とが対応付けて記憶されているが、この場合においても、記録情報として付加情報とセンシング情報とは一体化して記憶されていると云える。

【００４６】

以下に図５の説明を行う。情報種別は、いかにどのような情報が格納されてい

るかを示すものである。例えばマーケティングなどに情報を活用しようとする情報利用者は、この種別をもとに、以下の情報は自分が利用したい情報かどうかを即座に判断することができる。アクセス権は、格納されている情報の利用者（情報利用者）を限定するために、格納されている情報に応じて、予め定められているものである。この場合には、生体情報であるので、いずれもアクセス権は高く、アクセス権として「低」、「中」、「高」と３段階のレベルに区別されている場合、最も高い「高」となっている。

【００４７】

地域ＩＤは、情報提供者がどの地域に住むのかを示す。暗号種別は、公開鍵暗号あるいは共通鍵暗号などの暗号化方法だけでなく、部分的に暗号化されていたり、全体が暗号化されていたり、複数の暗号化が組み合わさっている可能性がある。これらどのようになっているか、その種別を示すものである。ここでは、数値で、当該種別を表している。生体情報は匿名化すべき情報であるので、暗号化されて格納されている。各生体情報を提供した情報提供者の氏名、住所などの各個人特有の個人情報は、暗号化され、アクセス情報構造化記憶部３内に、図５に示したような生体情報や付加情報などからなる記録情報とは別個に記憶されている。

【００４８】

図６は、アクセス情報構造化記憶部３の個人情報の記憶例を説明するためのもので、各個人情報には、そのそれぞれを識別するためのＩＤ（個人ＩＤ）をもち、これを図６では、「Ｐ１」、「Ｐ２」、…と表している。図６では、簡単のため、各個人情報に個人ＩＤのみしか記述されていないが、実際には、各個人情報には、氏名や住所などの具体的な個々の個人情報も含まれている。

【００４９】

図６の個人情報と図５の生体情報とを対応付ける（関連付ける）のは、図５に示したような、各記録情報に与えられた暫定ＩＤである。暫定ＩＤと個人ＩＤ（個人情報のＩＤ（識別子））との対応付けは情報関連化部２２が行う。暫定ＩＤは、各記録情報に対しランダムに与えられ、暫定ＩＤと個人ＩＤとの対応関係は、情報関連化部２２のみが知っている。例えば、暫定ＩＤと個人ＩＤとの対応関

係は、情報関連化部２２に記録され、情報関連化部２２のみが読み出しできるようになっている。

【００５０】

図５に示した各記録情報のうち、情報種別、アクセス権、地域ＩＤ、性別、年齢、取得月日などは、ここでは、暗号化されていないので、特別なアクセス権がなくても（例えば、情報利用者のアクセス権が最低レベルでも）参照することが可能である。情報利用者は、データマイニングしたい対象に該当するかどうかを、これらの情報により、簡単に判断することができる。

【００５１】

図１の情報匿名化システムは、上記以外に、さらに、情報提供者側から送信されてきた上記センシング情報などの記録要求や、情報提供者から提供されてアクセス情報構造化記憶部３内に記録したセンシング情報などを利用するための情報利用者からのアクセス要求などを受信したり、当該アクセス要求に対応した情報をアクセス要求元の情報利用者への送信などを行う送受信部４と、送受信部４で受信した情報利用者側から送信された認証情報を認証するための認証部５と、認証部５で認証された情報利用者のアクセス権に応じてアクセス構造化情報記憶部３に記憶された情報のうち匿名化すべき部分に対する加工を行う情報匿名化部７を具備している。

【００５２】

アクセス情報追加部２の情報匿名構造化部２３は、情報提供者から提供された（送られてきた）情報から、秘匿すべき（匿名化すべき）情報と、そうでない情報とを分離する。

【００５３】

図７は、センシング部１で得た情報（例えば、ここでは、生体情報）をアクセス構造化情報記憶部３に（匿名化して）記憶するまでの、情報匿名化システムの処理動作を説明するための図である。

【００５４】

例えば、図３に示したような端末からなるセンシング部１が、当該端末から生体情報を取得し、通信部１５を介して、図４のような生体情報を送受信部４に送

る場合を例にとり説明する。この場合、生体情報を送信に先立ち、センシング部１は、まず、認証情報を含む認証要求を送信する。この認証要求は送受信部４を介して認証部５に送される（ステップＳ１）。認証情報としては、例えば、情報提供者の指紋や顔写真、あるいは虹彩などの認証情報としての生体情報あるいはセンシング部１である図３に示したような端末自体に組み込まれているＩＣカードなどの認証データなどが考えられる。

【００５５】

認証部５は、認証要求に含まれる上記のような認証情報に基づいて、個人認証を行う。当該認証要求が正当な場合に、認証部５は、認証権ｘ１を情報関連部化２２に渡すとともに、センシング部１にも当該認証権ｘ１と同じ認証権ｘ２を返し（ステップＳ３、ステップＳ４）、認証要求が不正な場合には、認証部５は、認証権を与えることなく、その後の処理は中断される。

【００５６】

認証要求と並行して、センシング部１から送受信部４を介して、生体情報を情報匿名化システムへ記録するための情報記録要求と情報匿名化要求とが、送受信部４を介して情報関連化部２２に送られる（ステップＳ２）。情報関連化部２２は、認証部５での判定結果を受け取り、この判定結果が「正当」の時には、認証部５から送られてきた認証権ｘ１を保持し、次にセンシング部１から生体情報が送られてくるのを待つ。認証結果が「不正」のときには、センシング部１からの情報を待たずに、現時の情報記録要求と情報匿名化要求を破棄し、処理を中断する。

【００５７】

センシング部１は、認証結果が「正当」である旨を受け取って、与えられた認証権ｘ２と生体情報とをあわせて、通信部１５を介して、再度送受信部４に送る（ステップＳ５）。なお、センシング部１は、生体情報とともに、当該生体情報の提供者の氏名や住所や個人の識別子などの個人情報も送信するようにしてもよい。この個人情報は、例えば、センシング部１としての端末（例えば、図３のＰＤＡ）に予め登録されているものである。

【００５８】

以下、ここでは、生体情報とともに個人情報もセンシング部１から送信されるものとする。が、この場合に限らず、例えば、情報匿名化システムには、当該情報提供者の個人情報がアクセス構造化情報記憶部３に予め登録されており、センシング部１からは個人の識別子のみが送られ、この個人の識別子から、例えば、情報関連部２２が当該識別子に対応する個人情報を得て、センシング部１から送信されてきた生体情報に対応付けるようにしてもよい。

【００５９】

送受信部４は、生体情報と個人情報と認証権ｘ２を、情報関連化部２２に送る。情報関連化部２２は、保持している認証権ｘ１と、受け取った認証権ｘ２とが同一であるかどうかを判定する。

【００６０】

同一であったときには、当該認証権に基づき、個人情報ＩＤを生成する。生成した個人情報ＩＤに対応付ける暫定ＩＤをランダムに生成する（ステップＳ６）。生成した暫定ＩＤと、生体情報、個人情報、情報記録要求と情報匿名化要求をアクセス情報追加部２１に送る（ステップＳ７）。

【００６１】

なお、ここで個人情報とは、情報提供者の氏名や住所、その他、当該情報提供者のプライバシーに関わる非常に重要度の高い（秘匿性を要する）情報である。すなわち、この個人情報は、秘匿化すべき（匿名化すべき）情報として予め定められているものであり、アクセス権としては、最も高いレベル（好ましくは、生体情報に対するアクセス権よりも高いレベル）であるとする。

【００６２】

情報追加部２１は、暫定ＩＤに対し、生体情報へアクセス可能な情報利用者を限定するためのアクセス権のレベルを定めたレベル情報と、例えば、情報記録要求に含まれる情報（例えば、付加情報として付加するための情報）や必要に応じて、当該生体情報の情報提供者の個人情報などを参照して、図５に示すように、付加情報を生成するとともに、当該付加情報を生体情報に付加し、さらに個人情報とをまとめて記録情報として出力する。

【００６３】

暫定ＩＤと上記記録情報と情報記録要求と情報匿名化要求は、匿名化されるために、情報匿名構造化部２３に送られる（ステップＳ８）。

【００６４】

情報匿名構造化部２３は、記録情報のうち、匿名化すべき部分とそうでない部分を分離する。匿名化すべき情報とは、ここでは、生体情報と個人情報である。上記録情報のうち、生体情報と個人情報を除く他の情報は、匿名化する必要のない情報である。

【００６５】

記録情報に含まれる匿名化すべき情報のうち、個人ＩＤと統合すべきもの、すなわち、この場合上記個人情報は上記記録情報から分離し、匿名化すべき情報のうち、上記個人情報以外の情報（すなわち、ここでは、生体情報）を暗号化して、暫定ＩＤとともに、アクセス構造化情報記憶部３に送付する（ステップＳ９）。このとき、匿名化する必要のない情報もアクセス構造化情報記憶部３に送付する。

【００６６】

情報匿名構造化部２３では、記録情報から分離した個人情報は個人ＩＤと統合するために、暫定ＩＤとともに、情報関連化部２２に送る（ステップＳ１０）。情報関連化部２２は、予め記憶した暫定ＩＤと個人ＩＤの対応表をもとに、個人情報を個人ＩＤと統合し、当該個人情報を暗号化し、アクセス構造化情報記憶部３に送付する（ステップＳ１１）。

【００６７】

アクセス構造化情報記憶部３は、情報関連化部２２より送られてきた暗号化された個人情報と、情報匿名構造化部２３より送られてきた暗号化された生体情報と暫定ＩＤと秘匿する必要のない情報とを、それぞれ、例えば、図６、図５のような形式で記憶する（ステップＳ１２）。実際には、生体情報や個人情報は暗号化されているので、それらの内容は陽に可読な形式になっているわけではない。

【００６８】

アクセス構造化情報記憶部３は、匿名化情報を記録し終わると、その旨の応答を情報関連化部３２を介してセンシング部１に返す（ステップＳ１３）。

【００６９】

以上により、個人情報と個人情報以外のセンシング情報とは分離されて記録される。

【００７０】

以上の例では、生体情報それ自身には、個人を特定するものはなかった。しかし、センシング部１が図８のように、撮像部１６と通信部１５からなるような場合には、撮像部１６が取得した画像には、個人ＩＤなどの直接的な情報が含まれていないとしても、人物の顔などの個人情報が含まれている可能性がある。このようにセンシング部１がセンシングした情報自体に個人のプライバシーに関わるような秘匿すべき情報（個人情報）が含まれている場合に、これを抽出するのが、匿名抽出部２４である。

【００７１】

特開２０００－３１１２５１公報の段落番号「０１５５」から段落番号「０１５６」には、フラクタルを用いて、画像中から対象を切り出す手法について述べられている。例えば、図９、図１０に示すような２種類の抽出手法がある。

【００７２】

図１０は、Ｓｎａｋｅと呼ばれる手法で、対象物体の輪郭線（図では建物を囲む白い曲線）のエネルギーが最小になるようにするものである。この場合、図１０（ｂ）にあるように、エネルギー最小であるために、輪郭線は丸くなるので、建物のとがった部分などをうまく抽出できないという難点がある。

【００７３】

これに対し、図９に示すフラクタル(Fractal)手法は、フラクタル値（同様の形状の繰り返し度）を上げていくことで、鋭利な部分にも、追随することが可能である。従って、輪郭線は、Ｓｎａｋｅ手法に比較すると、図９（ｂ）に示すように、建物の尖った部分にもうまく追随して、抽出することが可能である。

【００７４】

例えばこのような抽出手法を用いて、図１１のように撮像した画像中から人物など、個人のプライバシーに関わる部分だけを切り出すことが可能である。

【００７５】

図１２は、図１１に示した画像を処理対象として、匿名抽出部２４によって抽出された個人情報としての人物の画像情報（図１２（ａ））と、抽出された当該個人情報を秘匿するために当該人物の画像情報を削除する、あるいは、モザイクをかけるなどの加工を施して、匿名化された情報（図１２（ｂ））、すなわち、匿名化情報を示している。

【００７６】

図１３は、情報匿名化システムの、匿名抽出部２４にて秘匿情報を抽出する場合の、センシング部１で得た個人情報を含む情報（例えば、ここでは、画像情報）をアクセス構造化情報記憶部３に（当該秘匿情報を匿名化して）記憶するまでの、情報匿名化システムの処理動作を説明するための図である。ここでは、画像情報中の個人情報は、個人の画像である。従って、この場合、センシング部１でセンシング情報として取得した画像中に個人情報が予め含まれている場合であって、これは、図７において、センシング部１でセンシング情報として取得した生体情報中の一部が個人情報である場合と同様である。従って図１３のステップＳ１からステップＳ８までの処理は、図７と同様なので説明は省略する。

【００７７】

ここでは、図１３のステップＳ８以降について説明する。すなわち、ステップＳ８において、暫定ＩＤと、付加情報と上記個人情報を含む画像情報などからなる記録情報と、情報記録要求と、情報匿名化要求は、情報匿名構造化部２３に送られると、さらに、当該記録情報と暫定ＩＤは、当該記録情報から個人情報を抽出するための要求とともに匿名抽出部２４へ送られる（ステップＳ９ａ）。匿名抽出部２４では、記録情報中の画像情報から、上記フラクタル法などを用いて人物の画像部分、すなわち、匿名化すべき情報（個人情報）を抽出する（ステップＳ９ｂ）。この抽出された匿名化すべき情報（人物の画像部分）と暫定ＩＤとは、情報匿名構造化部２３に渡される。これを受けて、情報匿名構造化部２３では、個人情報として抽出された人物の画像と暫定ＩＤとを個人ＩＤと統合するために、暫定ＩＤとともに、情報関連化部２２に送る（ステップＳ１０）。

【００７８】

記録情報中の画像情報のうち、抽出された個人情報を除く部分は、この時点に

おいて、情報匿名化部において、当該個人情報に対応する部分を削除したり、モザイクをかけたり、あるいは、他の情報と置き換えるなどの匿名化のための加工を行うようにしてもよい。このようにして匿名化処理の施された情報、すなわち、匿名化情報は、アクセス構造化情報記憶部３へ渡す。なお、この匿名化情報は暗号化してもよい。また、アクセス情報追加部２の情報追加部２１では、抽出された個人情報にアクセス可能な情報利用者を限定するためのアクセス権のレベルを定めたレベル情報が付加情報として付加する。

【００７９】

情報関連化部２２は、予め記憶した暫定ＩＤと個人ＩＤの対応表をもとに、個人情報を個人ＩＤと統合し、当該個人情報を暗号化し、アクセス構造化情報記憶部３に送付する（ステップＳ１１）。

【００８０】

アクセス構造化情報記憶部３は、情報関連化部２２より送られてきた暗号化された個人情報と、情報匿名構造化部２３より送られてきた匿名化情報（暗号化されていてもよい）と暫定ＩＤを、それぞれ、例えば、図５、図６のような形式で記憶する（ステップＳ１２）。その後、記録終了の応答をセンシング部１へ返す（ステップＳ１３）。

【００８１】

次に、情報利用者から情報利用の要求があった場合の情報匿名化システムの処理動作について、図１４を参照して説明する。

【００８２】

情報利用者は例えば、ＰＣ作業における集中度が、１週間の作業時間に応じて、どのように変化しているかを知りたいとする。集中度はＧＳＲの値で知ることができるので、例えば、次のような検索要求文をＸＭＬ(extensible Markup Language)形式などで記述して送る。

｛カテゴリ：男性＆女性、項目１：ＰＣ作業時間／週、項目２：集中度｝

なお、上記検索要求文は、情報利用者の端末側にて、あるいは、上記検索要求文を受信した情報匿名化システムの例えば情報管理部６などで、上記検索要求文中の検索すべき情報の種類を表す「項目」の名称を、実際にアクセス構造化情報

記憶部３に記憶されている情報の種類を表す名称に変換するなどして、検索要求文自体を情報匿名化システムに適合するように変換してもよい。例えば、上記検索要求文の場合、

｛カテゴリ：男性＆女性、項目１：ＰＣ作業時間／週、項目２：ＧＳＲ｝

となる。

【００８３】

情報利用者の端末が上記検索要求文を含む情報利用要求を出す際、まず、これに先立ち、認証情報を含む認証要求が送受信部４を経て、認証部５に送られる（ステップＳ２１）。その後、上記情報利用要求を送信する（ステップＳ２２）。認証部５では、情報利用者が情報利用が認められているものであるかどうかを確認する。情報利用の認証許可は別途設けられる認証局によって与えられる。認証許可が与えられた情報利用者は、与えられた公開鍵により、認証を行う。

【００８４】

公開鍵が正しくない場合には、認証部５は、認証権を与えないので、情報利用者は、それ以上の情報利用を行うことはできない。

【００８５】

認証部５で情報利用者の認証が成功すると、当該情報利用者に対し予め定められたアクセス権のレベルを定めたレベル情報を含む認証権を送信部４へ渡す（ステップＳ２３）。あるいは、当該認証権を送信部４を介して情報利用者の端末へ一度送信し、それが送り返されて当該認証権を受信するようにしてもよい（ステップＳ２４）。

【００８６】

送信部４は、情報利用者が送ってきた情報利用要求と、認証部５から戻ってきた（あるいは情報利用者の端末から送信された）認証権を一緒にして、情報匿名化部７に送る（ステップＳ２５）。

【００８７】

情報匿名化部７は、受け取った情報利用要求をもとに、要求のあった情報（例えば、情報利用要求に含まれる上記検索要求文に合った情報）を読み出すべく、情報読み出し要求をアクセス構造化情報記憶部３に送る（ステップＳ２６）。ア

クセス構造化情報記憶部３では、図５、図６に示すように、匿名化すべき個人情報とそれ以外の情報がわかれて記憶されている。

【００８８】

なお、上記検索要求文のように、「カテゴリ」を指定した情報利用の場合には、個人情報は関係ないので、情報利用者のアクセス権のレベルに基づき、当該情報利用者に公開可能なレベルの情報を当該情報利用者に提供する。

【００８９】

カテゴリは「男性＆女性」なので、図５に示した各情報は、全てのこのカテゴリに当てはまるので、図５に示した情報（別個記録されている暗号化された生体情報を含む）を全て読み出して情報匿名化部７に送られる（ステップＳ２７）。

【００９０】

情報匿名化部７では、当該認証権に含まれるアクセス権のレベルに応じて、読み出した情報中に匿名化すべき情報があるときには、匿名化を行う。また、読み出した情報中に情報利用者に情報すべきでない情報がある場合には、その情報を削除する（ステップＳ２８）。例えば、図５に示した各情報では、すでに個人情報は分離されているので、匿名化する必要はないが、個人情報を関連付けるための暫定ＩＤは残っている。したがって、この例では、読み出した情報のうち、この暫定ＩＤを削除する。

【００９１】

なお、ここで、アクセス権とは、情報利用者毎に予め定められているものであり、情報利用者毎に、どのレベルの情報が利用可能であるかを特定するための情報である。上記例の場合、上記検索要求文から所望の情報を受け取ることのできる情報利用者は、少なくとも生体情報へのアクセスが予め許可されていることが必要であり、生体情報へのアクセスが許可されてはいても、個人情報へのアクセスは許可されていなければ、当該生体情報が誰のものかまではしることはできない。一方、生体情報の情報提供者の主治医の場合は、当該情報提供者に限って、当該情報提供者の個人情報とともに生体情報へアクセス可能にするといったアクセス権を定めることもできる。

【００９２】

また、生体情報などの秘匿情報を記録する際に、当該記録対象の秘匿情報に定めたアクセス権（「低」、「中」、「高」）を、情報利用者のアクセス権に用いてもよく、例えば、生体情報のアクセス権が「中」である場合には、生体情報にアクセスすることができる情報利用者のアクセス権は、「中」、あるいは「中」と「高」のうちのいずれかである必要があると定めてもよい。また、個人情報にのアクセス権が「高」である場合には、個人情報にアクセスすることができる情報利用者のアクセス権は、「高」である必要があると定めてもよい。

【００９３】

さて、情報匿名化部７にて必要な処理の施された情報（匿名化情報）は、情報利用者の端末に向けて送信される（ステップＳ２９）。

【００９４】

情報利用者の端末では、情報匿名化情報から送信されてきた上記匿名化情報を受け取ると、例えば図１５にあるように、当該匿名化情報中のデータをまとめて、週当たりのＰＣ作業時間と、その行為を行っている行為者の率、全体の平均集中度、男性のみの集中度をレポートにすることができる。

【００９５】

情報利用者は、情報利用の対価を課金管理部に支払う（ステップＳ３０）。課金管理部は、情報利用の許認可を行う認証局が兼ね、情報提供量に応じて、情報提供者に個別に割戻しを行うことも可能である。あるいは、課金管理部は、情報提供者が契約している金融機関が兼ね、そこに送金することも可能である。

【００９６】

なお、前述した画像情報のような情報利用要求を行う場合、画像情報には、記録時に予め匿名化処理が施されて記録されている。従って、情報利用者に対し予め与えられたアクセス権のレベルでは、当該画像情報中の個人情報にアクセス不可能なときには、匿名化情報のみを提供する。また、情報利用者に対し予め与えられたアクセス権のレベルで、当該画像情報中の個人情報にアクセス可能なときには、匿名化情報を読み出すとともに、当該匿名化情報（の暫定ＩＤ）に対応する個人情報のＩＤ（個人ＩＤ）を情報関連化部２２に記憶されている対応関係（対応表）から求めて、アクセス構造化情報記憶部３から当該個人情報を読み出す

。そして、例えば、情報匿名化部７では、当該個人情報を匿名化情報に合成して、再び、元の画像情報を生成して、これを送受信部４を介して当該情報の要求元である情報提供者へ送信する。あるいは、情報匿名化部７は、匿名化情報中の加工した部分、すなわち、個人情報に対応する部分を元の状態に戻すなどの加工を行う。

【００９７】

上記の実施形態では、センシング部１は端末として独立しており、ホームサーバーなどに組み込まれた情報匿名化システムと無線で送受信をおこなっていた。本発明はこのような構成に限定されるわけではない。小型デバイス技術の進展により、現在のホームサーバのように大容量のメモリサイズを有することが可能となると、図１６のように、センシング部１が情報匿名化システムに組み込まれた形で、携帯することも可能となる。

【００９８】

なお、図１６において、図１と同一部分には同一符号を付し、異なるのは、センシング部１が情報匿名化システムに組み込まれている点が異なるだけである。

【００９９】

また、上記実施形態では、医療機関などが情報利用者として、個人が情報提供者である場合を取り上げた。しかし、必ずしもこれに限定されるものではない。例えば、個人が情報利用者で、警察などが情報提供者である場合もある。

【０１００】

例えば、歌舞伎町の現在の様子を個人がしりたいと思ったときに、歌舞伎町の街角に設置されたカメラの映像を見たいとする。個人は、

｛カテゴリ：なし、項目１：歌舞伎町、項目２：リアルタイム｝

といった検索要求文を含む情報利用要求を出す。歌舞伎町のカメラを管轄している警察庁では、匿名抽出部２４をもちいて、個人情報に関わる例えば、顔の部分の画像情報を除いて、例えば、図１７のように匿名化された画像情報を提供する。

【０１０１】

以上説明したように、上記実施形態によれば、人物の顔などを含む映像情報、

脈拍や体温などの生体情報などの第１の情報を取得したら、当該第１の情報に、少なくとも当該第１の情報にアクセス可能な情報利用者を限定するためのアクセス権のレベルを定めたレベル情報を含む付加情報を付加して、当該第１の情報を提供した情報提供者に関する個人情報とは別個に記憶し、当該第１の情報と、当該第１の情報に対応する個人情報との間の対応関係も別に記憶する。記憶された第１の情報および当該第１情報に対応する個人情報のうちの少なくとも一方へアクセスするためのアクセス要求を受信したとき、当該アクセス要求の要求元である情報利用者に対し予め定められたアクセス権のレベルが第１の情報にアクセス可能なときには当該第１の情報を提供し、当該アクセス権のレベルが前記個人情報にアクセス可能なときには、別個記憶された対応関係に基づき、当該個人情報を読み出して当該個人情報も提供する。

【０１０２】

また、個人情報を含む第１の情報を取得して、当該第１の情報から個人情報を抽出し、当該第１の情報から抽出した個人情報を分離することにより、匿名化情報を生成し、この生成された匿名化情報に、少なくとも当該匿名化情報に対応する個人情報にアクセス可能な情報利用者を限定するためのアクセス権のレベルを定めたレベル情報を含む付加情報を付加して記憶するとともに、これとは別個に個人情報を記憶し、匿名化情報と当該匿名化情報に対応する個人情報との間の対応関係も別に記憶する。記憶された第１の情報のへアクセスするためのアクセス要求を受信したとき、当該アクセス要求の要求元である情報利用者に対し予め定められたアクセス権のレベルが個人情報にアクセス不可能なときには、当該アクセス要求に対応する第１の情報の匿名化情報を読み出して、当該匿名化情報を提供し、当該アクセス権のレベルが個人情報にアクセス可能なときには、別個に記憶された対応関係に基づき、さらに、当該第１の情報に対応する個人情報を読み出して、当該個人情報と当該匿名化情報とから第１の情報を生成して当該第１の情報を提供する。

【０１０３】

このように、生体情報や人物の画像などを取得した時点で、この取得した情報と、当該取得した情報とは別個に取得した個人情報とは分離して記憶する、ある

いは、当該取得した情報に含まれる個人のプライバシーに関わる情報（個人情報）は、個人情報でない情報と予め分離されて記憶されるので、後に情報利用者に個人情報以外の情報を提供する際には、提供した情報からは個人情報を辿っていくことが不可能である。従って、個人情報に関連付けられた情報であっても、他人からは当該個人情報にアクセスされることなく、当該情報の利用が可能となり、個人のプライバシーを守って情報利用を容易に行うことができるので、医療機関などの研究開発に寄与大である。なお、個人情報や生体情報などの情報に対し予めアクセス権を定めることにより、これら情報に対してもアクセス可能なレベルのアクセス権を有する情報利用者は、個人情報も参照することができる。

【０１０４】

従って、個人情報などの重要な情報はみだりに他人に公開されることなく保護しながら、一方で、匿名化された情報の利用の活性化が図れ、データマイニングが容易に効率よく行える情報共有環境が実現できる。

【０１０５】

（第２の実施形態）

第２の実施形態は図１７に示すように、第１の実施形態にて説明した情報匿名化システム１００を用いた情報利用サービスの仕組みを説明するためのものである。

【０１０６】

図１７において、上記第１の実施形態に係る情報匿名化システム１００は、情報提供者であるユーザに装着されたセンシング部１を通じて、生体情報や画像などの情報を取得し、上記第１の実施形態で説明したように、取得した情報から秘匿情報を分離して記憶する。

【０１０７】

一方、情報利用者である医師などの端末から送信される検索要求文を含む情報利用要求は、代理エージェントのサーバ装置にて受信される。当該情報利用要求は、当該サーバ装置を経由いて情報匿名化システムに対し情報利用提供を行い、その結果得られた、匿名化情報を基に、例えば、図１５に示したような、上記検索要求文に適したレポートを作成する。

【０１０８】

代理エージェントは、情報提供者に対し、当該情報提供者が提供した情報に対する情報提供料を支払うとともに、情報利用者に対しては、当該情報を利用したことに対する情報利用料を徴収する。

【０１０９】

このようなシステムを用いて実施される情報提供サービスによれば、個人情報を含む情報であっても、個人情報は匿名化してから情報を提供するので、各個人から提供された個人情報などの秘匿すべき情報を含む情報であっても円滑にしかも有効に他者に利用させることができる。

【０１１０】

本発明の実施の形態に記載した本発明の手法は、コンピュータに実行させることのできるプログラムとして、磁気ディスク（フロッピーディスク、ハードディスクなど）、光ディスク（ＣＤ－ＲＯＭ、ＤＶＤなど）、半導体メモリなどの記録媒体に格納して頒布することもできる。

【０１１１】

なお、本発明は、上記実施形態に限定されるものではなく、実施段階ではその要旨を逸脱しない範囲で種々に変形することが可能である。さらに、上記実施形態には種々の段階の発明は含まれており、開示される複数の構成用件における適宜な組み合わせにより、種々の発明が抽出され得る。例えば、実施形態に示される全構成要件から幾つかの構成要件が削除されても、発明が解決しようとする課題の欄で述べた課題（の少なくとも１つ）が解決でき、発明の効果の欄で述べられている効果（のなくとも１つ）が得られる場合には、この構成要件が削除された構成が発明として抽出され得る。

【０１１２】

【発明の効果】

以上説明したように、本発明によれば、個人情報を含む情報や、各個人に関わる個人情報に対応付けられた当該個人情報に準ずる生体情報や購買情報などの情報を個人情報を保護しつつ、各種目的で他人に有効に利用させることができる。

【図面の簡単な説明】

【図１】

本発明の第１の実施形態に係る情報匿名化システムの構成例を概略的に示した図。

【図２】

図１のセンシング部に対応する端末の外観を示した図。

【図３】

図１のセンシングの概略構成を示した図。

【図４】

生体情報の具体例を示した図。

【図５】

アクセス構造化情報記憶部における生体情報と付加情報の記憶例を示した図。

【図６】

アクセス構造化情報記憶部における個人情報の記憶例を示した図。

【図７】

図１の情報匿名化システムの情報記録時の処理動作を説明するための図。

【図８】

図１のセンシング部の他の構成例を示した図。

【図９】

取得した情報から個人情報に対応する情報部分を抽出するための手法を説明するための図。

【図１０】

取得した情報から個人情報に対応する情報部分を抽出するための他の手法を説明するための図。

【図１１】

センシング部で取得した情報であって、個人情報を含む画像情報の具体例を示した図。

【図１２】

（ａ）図は、図１１に示した画像中に含まれる個人情報を示した図であり、（ｂ）図は図１１に示した画像から個人情報を削除した結果得られる匿名化情報を

示した図。。

【図１３】

図１の情報匿名化システムの情報記録時の他の処理動作を説明するための図。

【図１４】

図１の情報匿名化システムの情報利用時の処理動作を説明するための図。

【図１５】

図１の情報匿名化システムから提供された情報を基に作成されたレポートの一例を示した図。

【図１６】

本発明の第１の実施形態に係る情報匿名化システムの他の構成例を概略的に示した図。

【図１７】

匿名化情報の一例を示した図。

【図１８】

第１の実施形態にて説明した情報匿名化システムを用いた情報利用サービスの仕組みを説明するための図。

【符号の説明】

１…センシング部

２…アクセス情報追加部

３…アクセス構造化情報記憶部

４…送受信部

５…認証部

６…情報管理部

７…情報匿名化部

２１…情報追加部

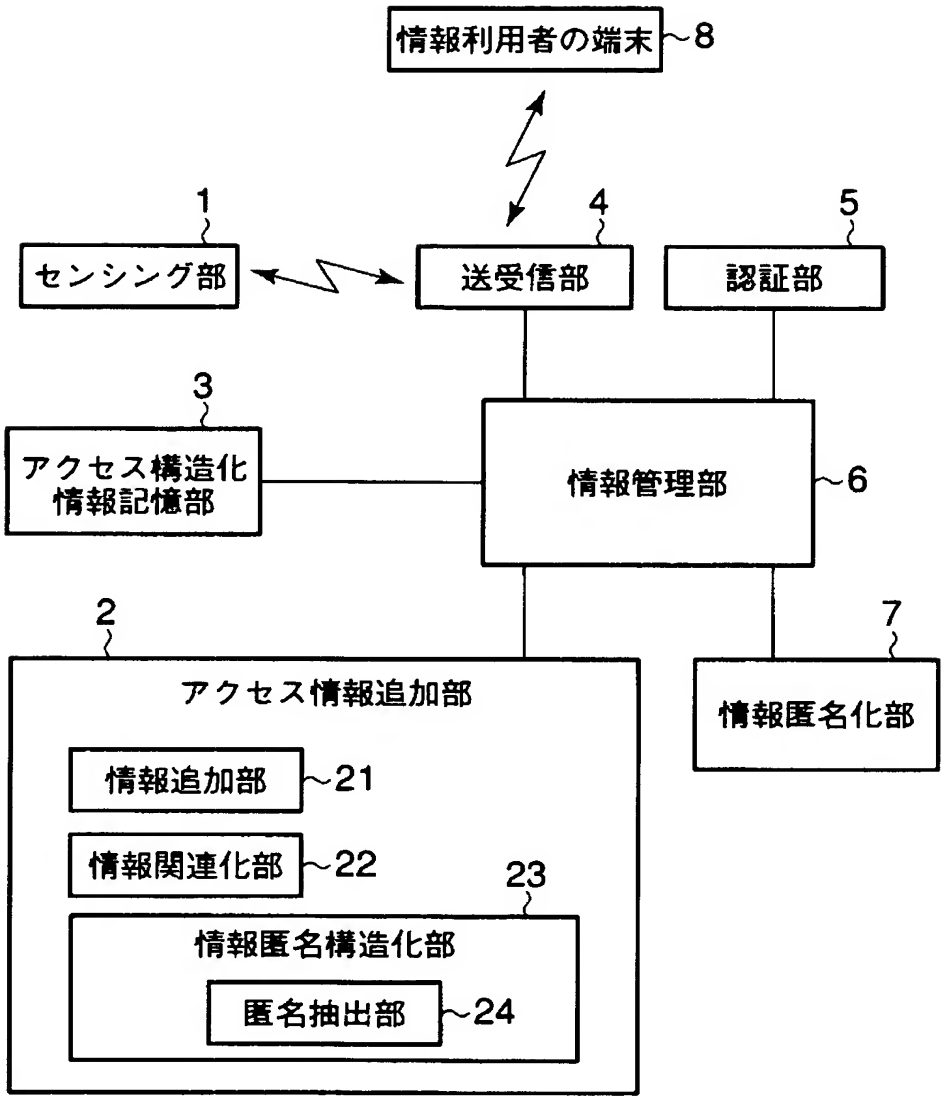
２２…情報関連化部

２３…情報匿名構造化部

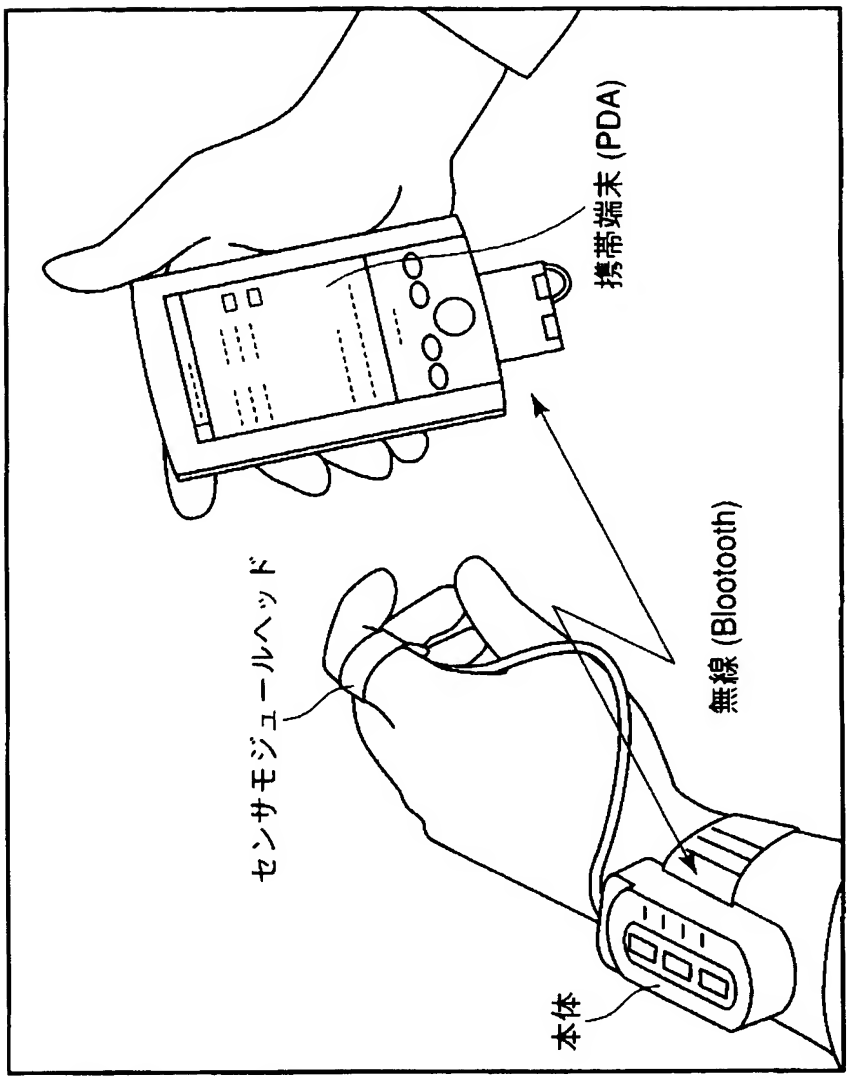
２４…匿名抽出部

【書類名】　図面

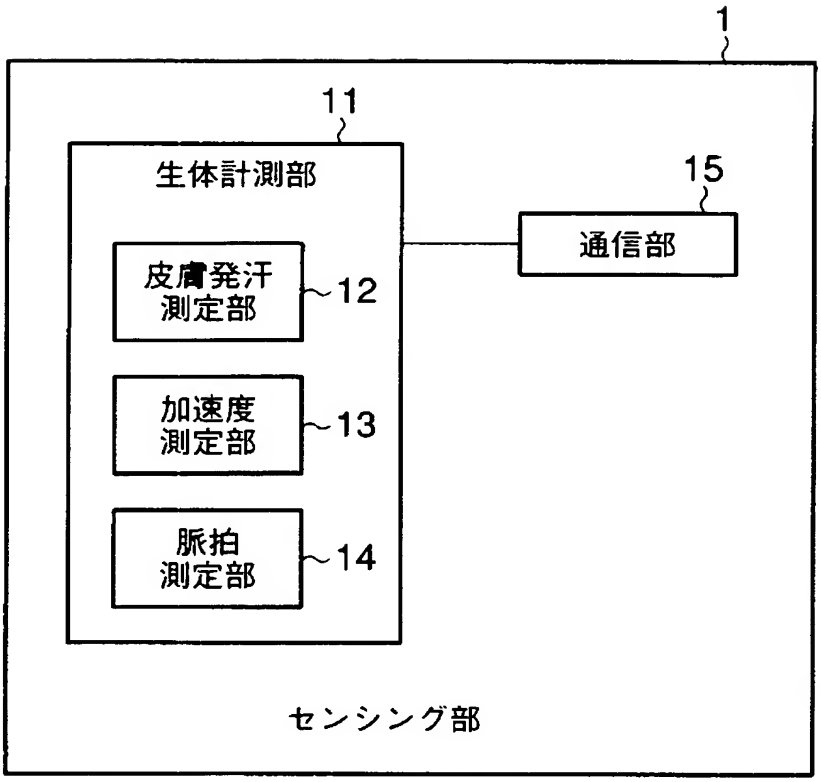
【図１】


情報利用者の端末
8
1
4
5
センシング部
送受信部
認証部
3
アクセス構造化
情報記憶部
情報管理部
6
2
7
アクセス情報追加部
情報匿名化部
情報追加部
21
情報関連化部
22
23
情報匿名構造化部
匿名抽出部
24

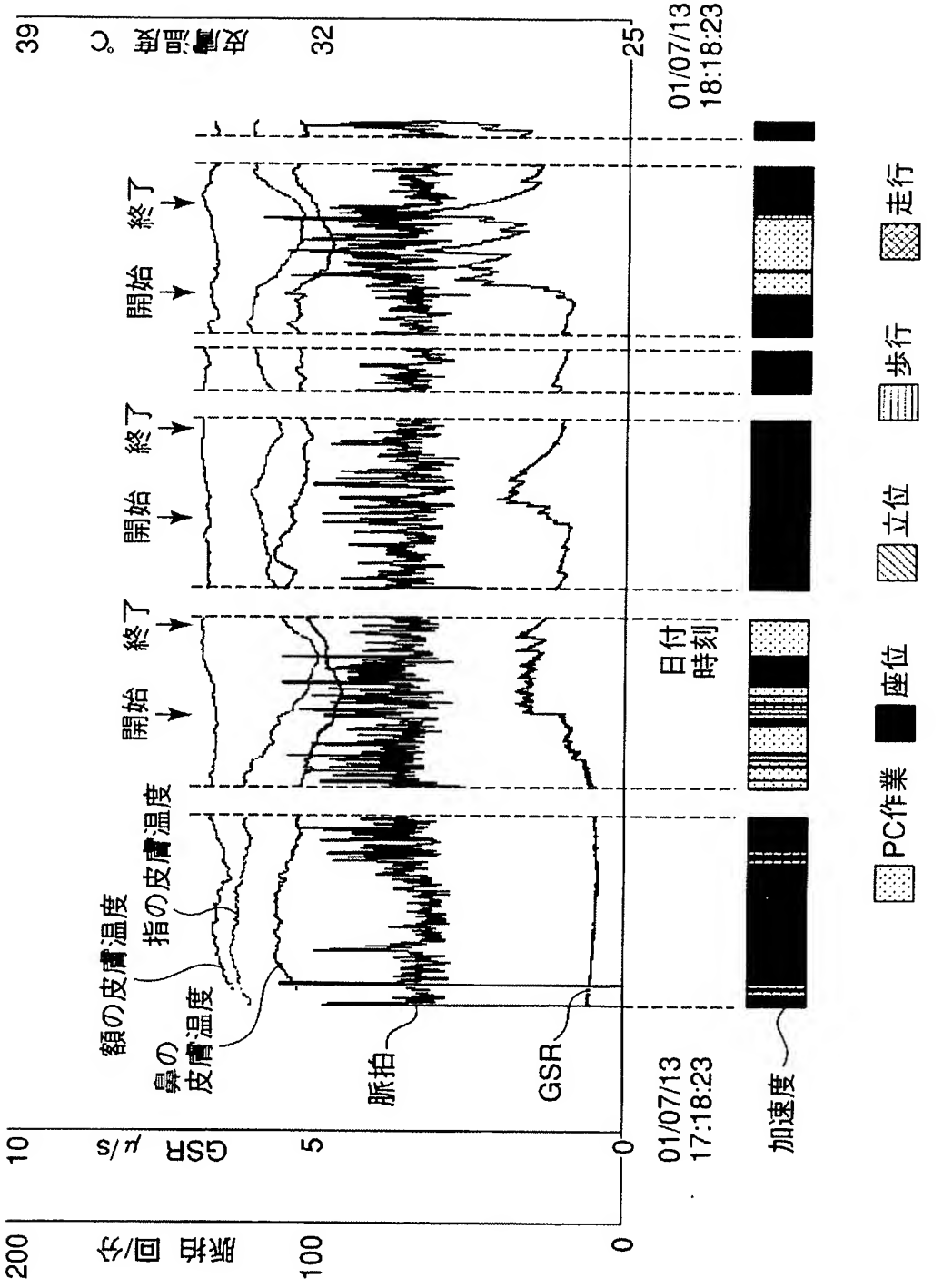
【図２】



【図３】



【図４】


皮膚温度 ℃
39
32
25
01/07/13
18:18:23
開始
終了
額の皮膚温度
指の皮膚温度
鼻の皮膚温度
脈拍
GSR
日付
時刻
01/07/13
17:18:23
加速度
脈拍 回/分
200
100
0
GSR μs
10
5
0
PC作業
座位
立位
歩行
走行

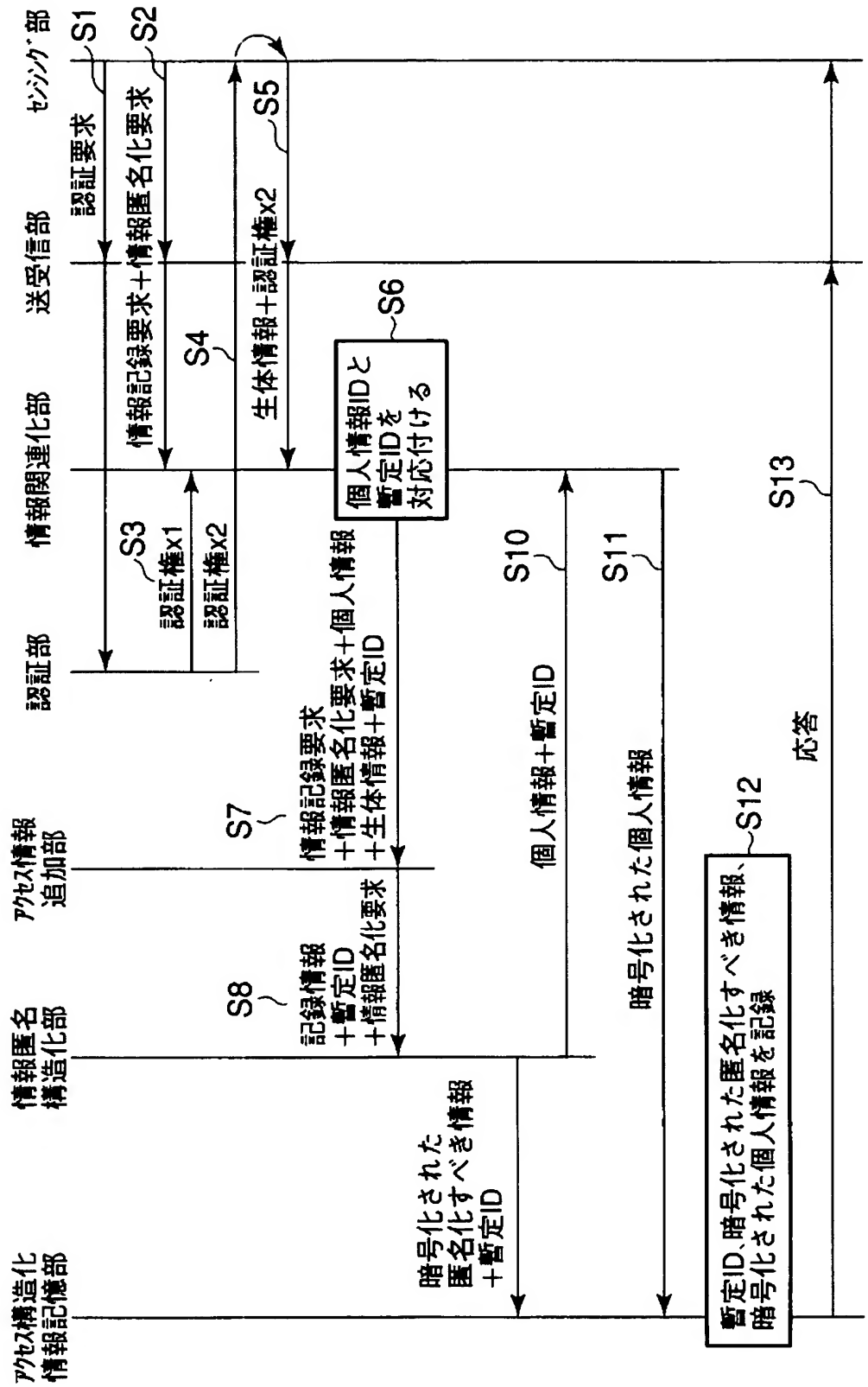
【図５】

暫定ID	情報種別	ｱｸｾｽ権	地域ID	暗号化種別	性別	年齢	情報取得日	生体情報
ID1	脈拍、GSR,体温、加速度、行動	高	984562	18	女性	38	2002/09/10	B1
ID2	脈拍、GSR,体温、加速度、行動	高	984562	18	男性	55	2002/09/10	B2
ID3	脈拍、GSR,体温、加速度、行動	高	984562	10	男性	50	2002/09/10	B3
ID4	脈拍、GSR,体温、加速度、行動	高	984562	10	女性	61	2002/09/10	B4
：		：	：	：	：	：	：	：

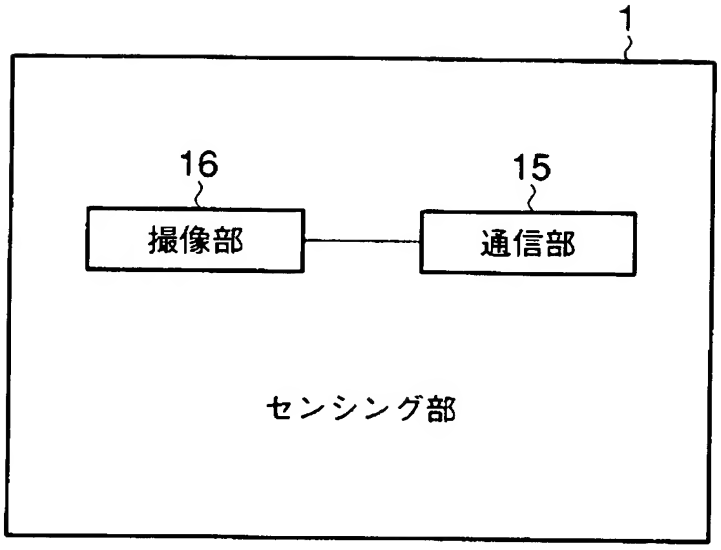
【図６】

個人情報
P1
P2
P3
P4
：

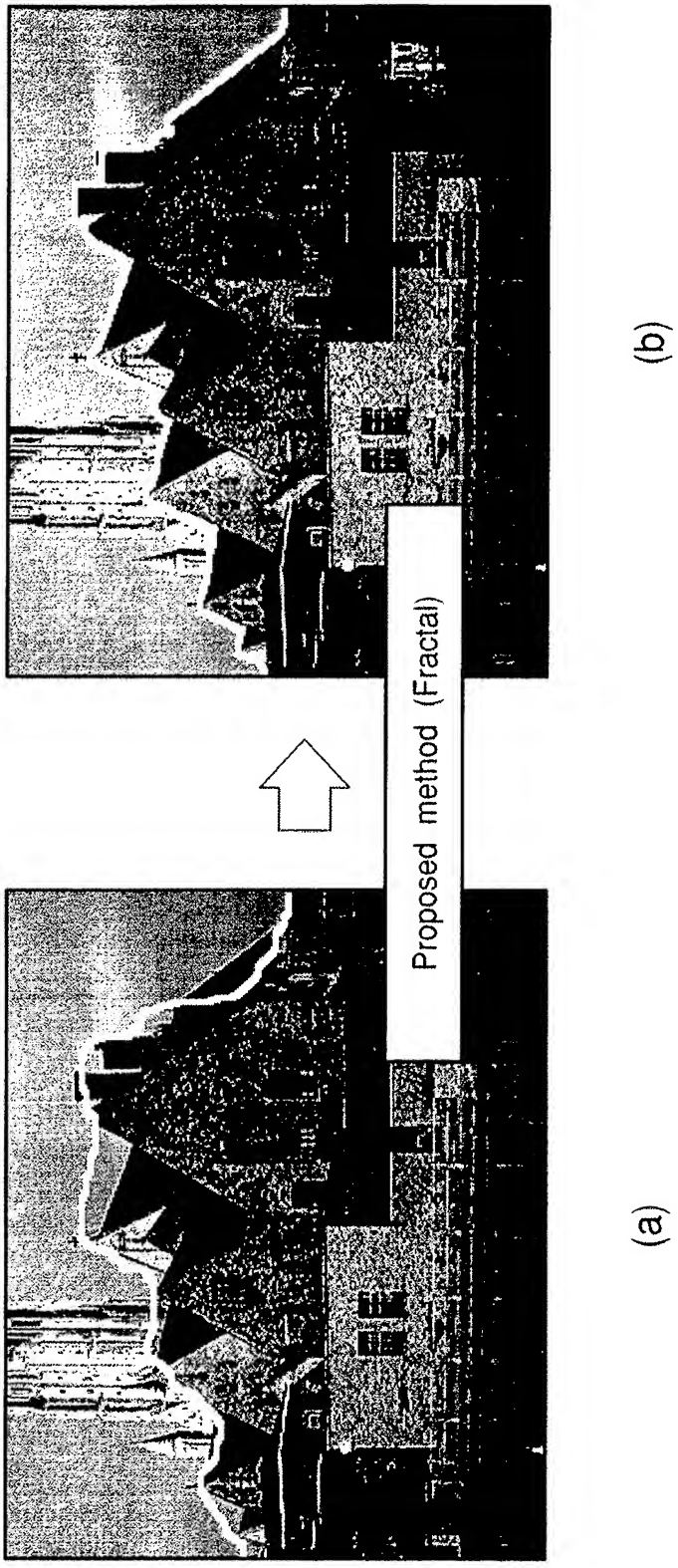
【図７】


センシング部
送受信部
情報関連化部
認証部
アクセス情報
追加部
情報匿名
構造化部
アクセス構造化
情報記憶部
S1
認証要求
S2
情報記録要求＋情報匿名化要求
S3
認証権x1
認証権x2
S4
S5
生体情報＋認証権x2
S6
個人情報IDと
暫定IDを
対応付ける
S7
情報記録要求
＋情報匿名化要求＋個人情報
＋生体情報＋暫定ID
S8
記録情報
＋暫定ID
＋情報匿名化要求
暗号化された
匿名化すべき情報
＋暫定ID
S10
個人情報＋暫定ID
S11
暗号化された個人情報
S12
暫定ID、暗号化された匿名化すべき情報、
暗号化された個人情報を記録
S13
応答

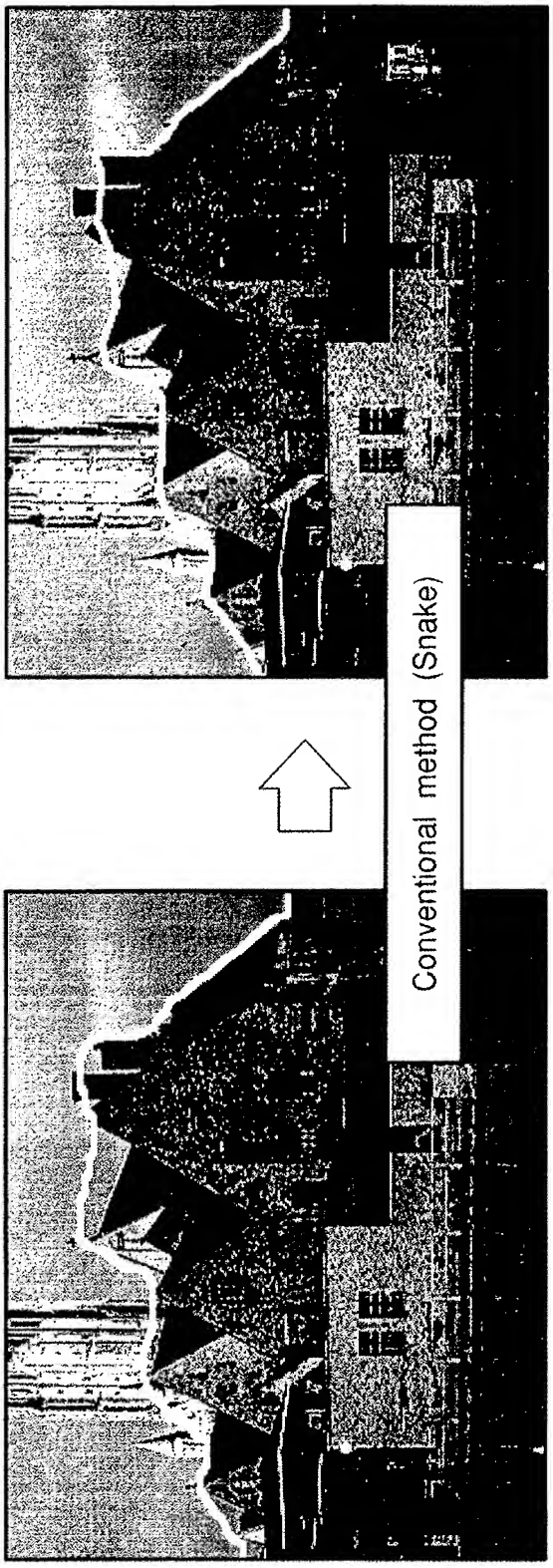
【図８】



【図９】

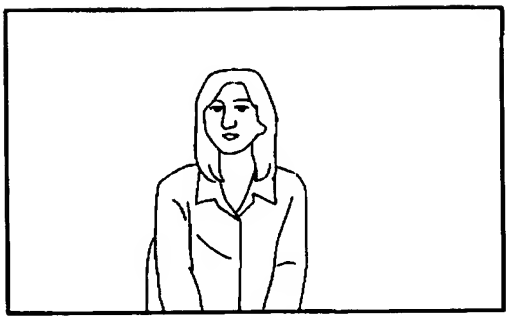


【図１０】



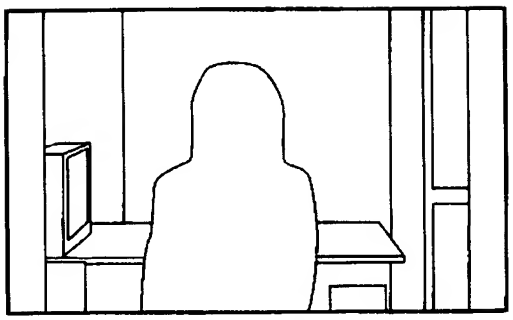
【図１１】

【図１２】



個人情報

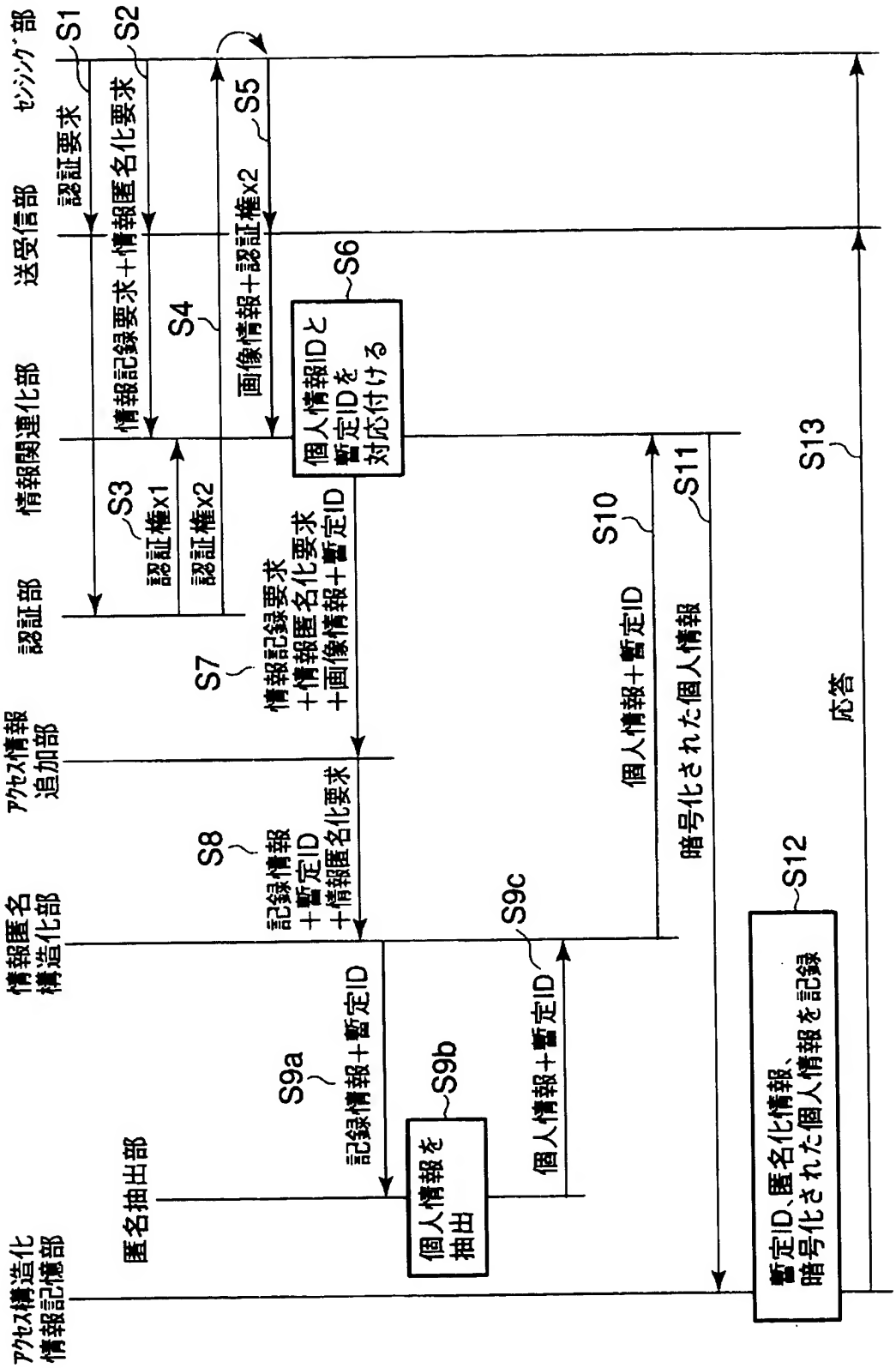
(a)



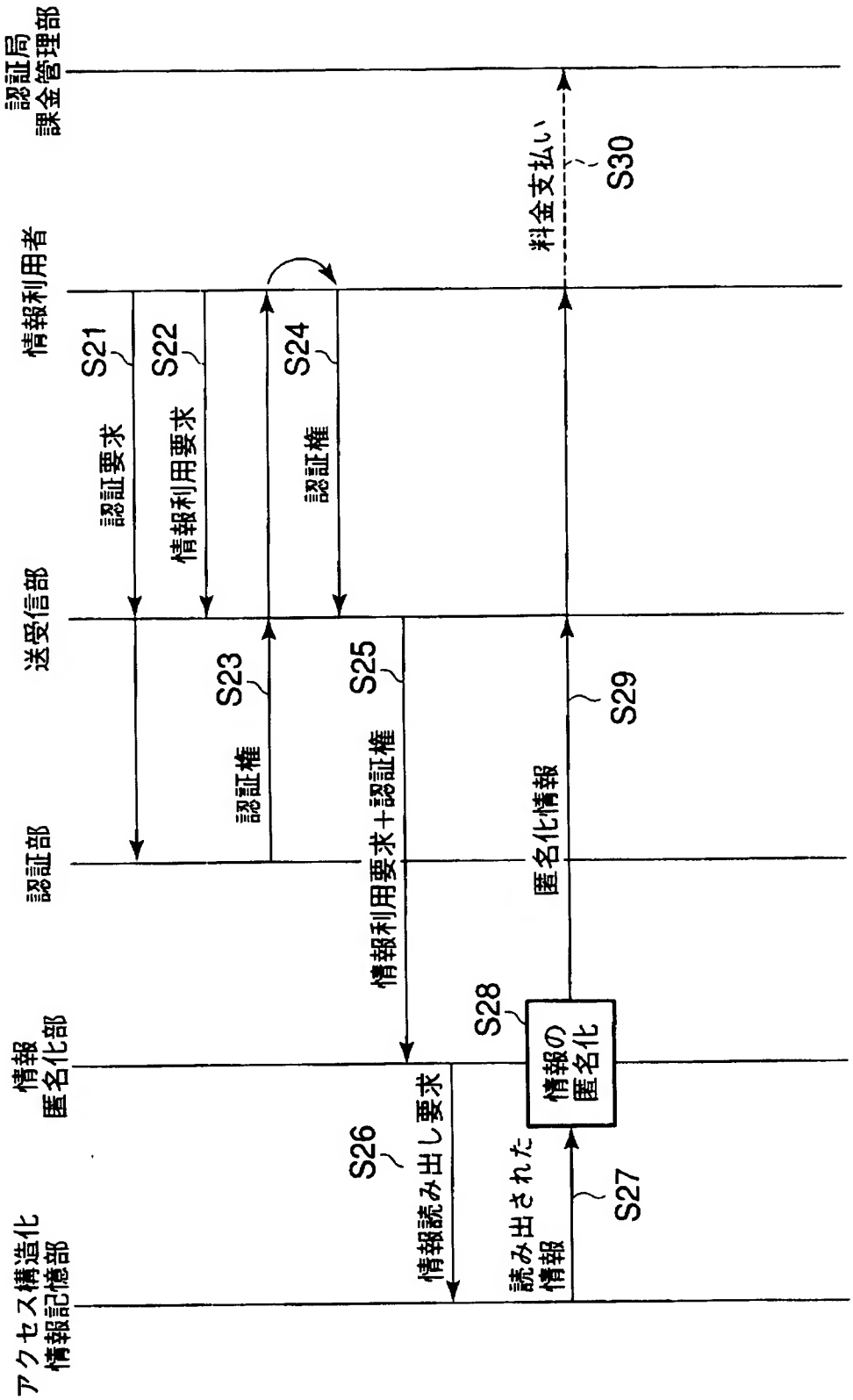
匿名化情報

(b)

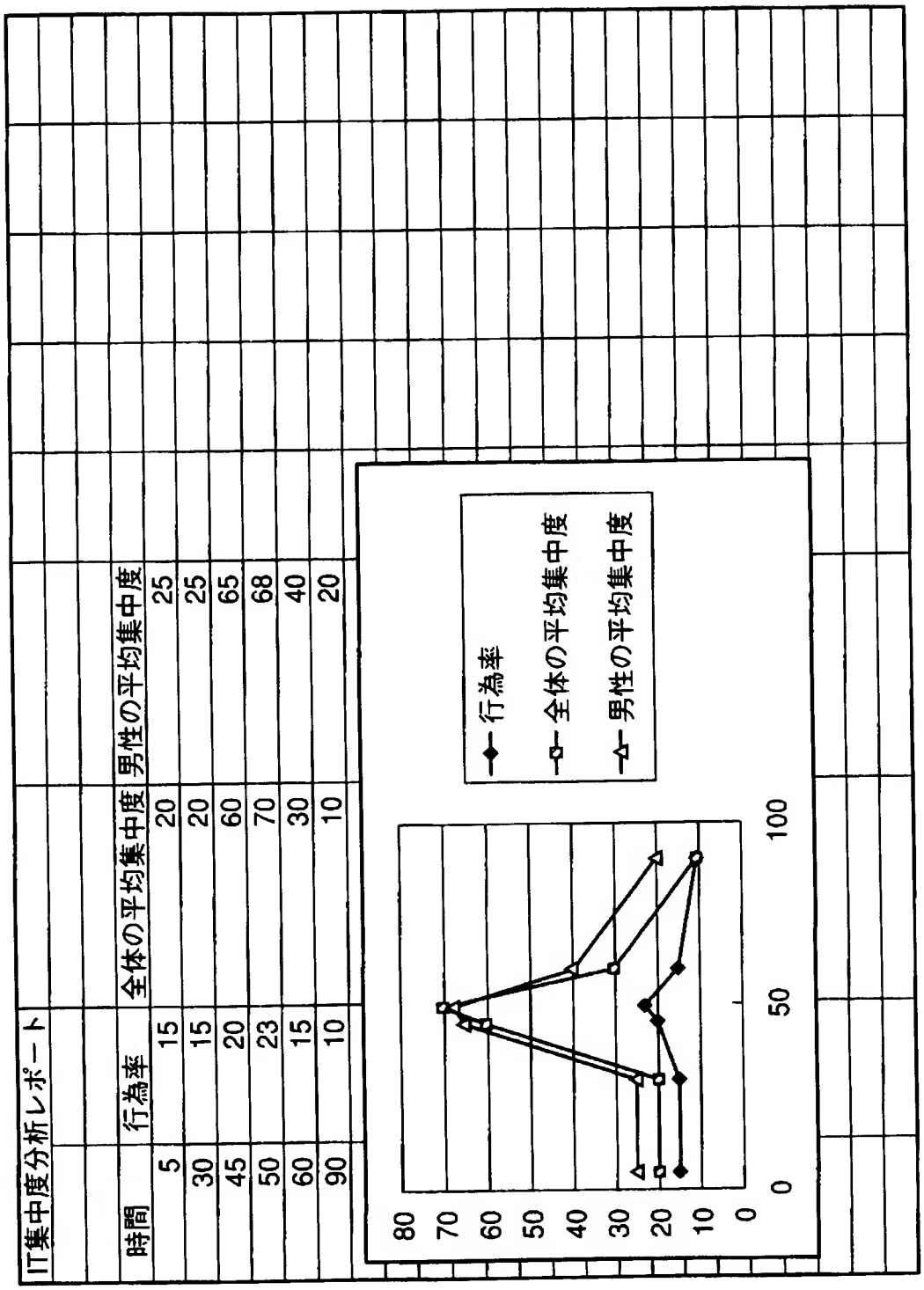
【図１３】


センシング部
送受信部
情報関連化部
認証部
アクセス情報追加部
情報匿名構造化部
匿名抽出部
アクセス構造化情報記憶部
S1
認証要求
S2
情報記録要求＋情報匿名化要求
S3
認証権x1
認証権x2
S4
画像情報＋認証権x2
S5
個人情報IDと暫定IDを対応付ける
S6
S7
情報記録要求＋情報匿名化要求＋画像情報＋暫定ID
S8
記録情報＋暫定ID＋情報匿名化要求
S9a
記録情報＋暫定ID
S9b
個人情報を抽出
S9c
個人情報＋暫定ID
S10
個人情報＋暫定ID
S11
暗号化された個人情報
S12
暫定ID、匿名化情報、暗号化された個人情報を記録
S13
応答

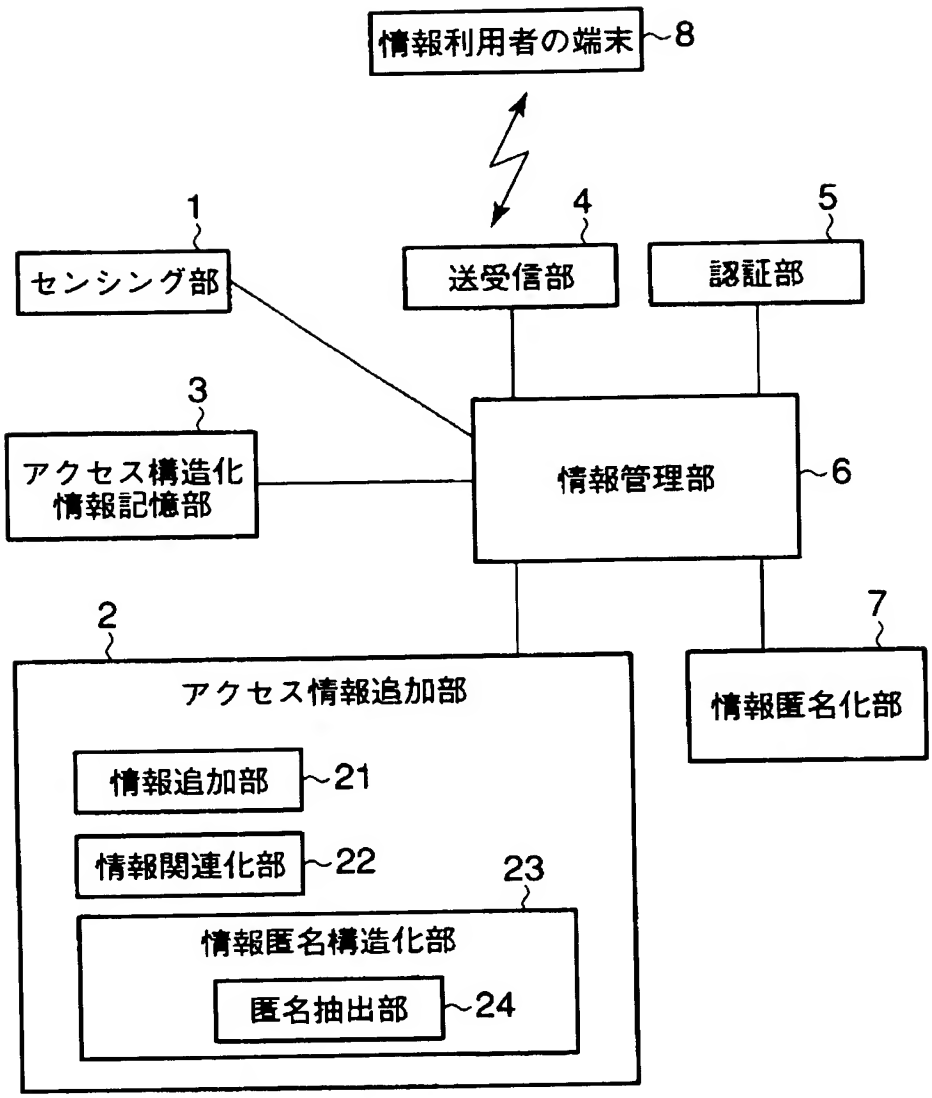
【図１４】


認証局
課金管理部
情報利用者
送受信部
認証部
情報
匿名化部
アクセス構造化
情報記憶部
S21
認証要求
S22
情報利用要求
S23
認証権
S24
認証権
S25
情報利用要求＋認証権
S26
情報読み出し要求
S27
読み出された
情報
S28
情報の
匿名化
S29
匿名化情報
S30
料金支払い

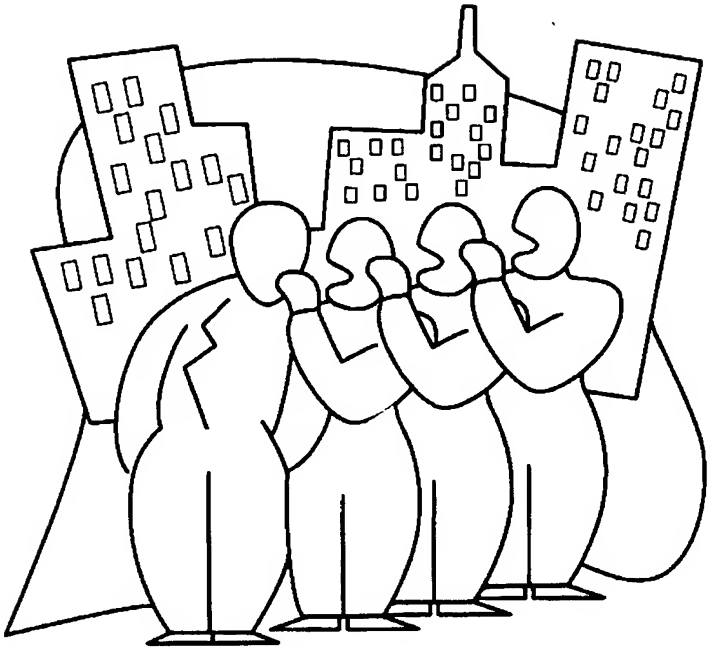
【図１５】


IT集中度分析レポート
時間
行為率
全体の平均集中度
男性の平均集中度
5 15 20 25
30 15 20 25
45 20 60 65
50 23 70 68
60 15 30 40
90 10 10 20
行為率
全体の平均集中度
男性の平均集中度
0 10 20 30 40 50 60 70 80
0 50 100

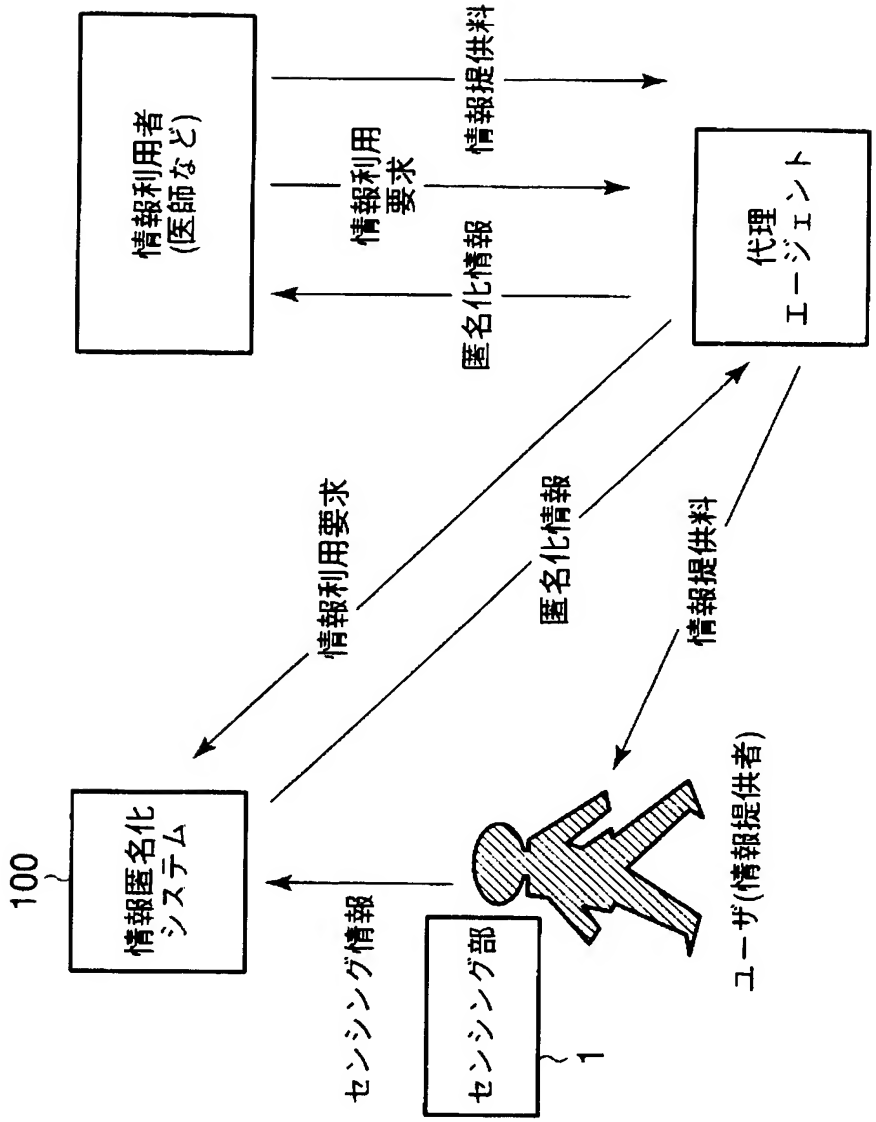
【図１６】


情報利用者の端末
8
1
センシング部
4
送受信部
5
認証部
3
アクセス構造化
情報記憶部
情報管理部
6
2
アクセス情報追加部
情報追加部
21
情報関連化部
22
23
情報匿名構造化部
匿名抽出部
24
7
情報匿名化部

【図１７】



【図１８】


情報利用者
(医師など)
情報利用
要求
情報提供料
匿名化情報
代理
エージェント
情報利用要求
匿名化情報
情報提供料
100
情報匿名化
システム
センシング情報
センシング部
1
ユーザ(情報提供者)

【書類名】　　要約書

【要約】

【課題】個人情報を含む情報や、各個人に関わる個人情報に対応付けられた当該個人情報に準ずる生体情報や購買情報などの情報を個人情報を保護しつつ、各種目的で他人に有効に利用させることができる情報共有支援装置を提供する。

【解決手段】人物の顔などを含む映像情報、脈拍や体温などの生体情報などの第１の情報を取得したら、当該第１の情報に、少なくとも当該第１の情報にアクセス可能な情報利用者を限定するためのアクセス権のレベルを定めたレベル情報を含む付加情報を付加し、これを当該第１の情報を提供した情報提供者に関する個人情報とは分離して記憶し、情報利用者に対し予め定められたアクセス権のレベルに応じた情報を提供する。

【選択図】　　図１

出　願　人　履　歴　情　報

識別番号　　［０００００３０７８］

１．変更年月日　　２００１年　７月　２日
［変更理由］　　住所変更
住　所　　東京都港区芝浦一丁目１番１号
氏　名　　株式会社東芝

２．変更年月日　　２００３年　５月　９日
［変更理由］　　名称変更
住所変更
住　所　　東京都港区芝浦一丁目１番１号
氏　名　　株式会社東芝